

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2003年12月18日 (18.12.2003)

PCT

(10) 国際公開番号
WO 03/104997 A1

(51) 国際特許分類: G06F 12/14, 17/60, G06K 17/00

[JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 Tokyo (JP).

(21) 国際出願番号: PCT/JP03/07250

(22) 国際出願日: 2003年6月9日 (09.06.2003)

(71) 出願人 および

(25) 国際出願の言語: 日本語

(72) 発明者: 坂村 健 (SAKAMURA, Ken) [JP/JP]; 〒141-0032 東京都品川区大崎4丁目9-2 Tokyo (JP). 越塚 登 (KOSHIZUKA, Noboru) [JP/JP]; 〒180-0013 東京都武蔵野市西久保2丁目27-20 Tokyo (JP).

(26) 国際公開の言語: 日本語

(30) 優先権データ:

特願2002-169241 2002年6月10日 (10.06.2002) JP

特願2002-169244 2002年6月10日 (10.06.2002) JP

(72) 発明者; および

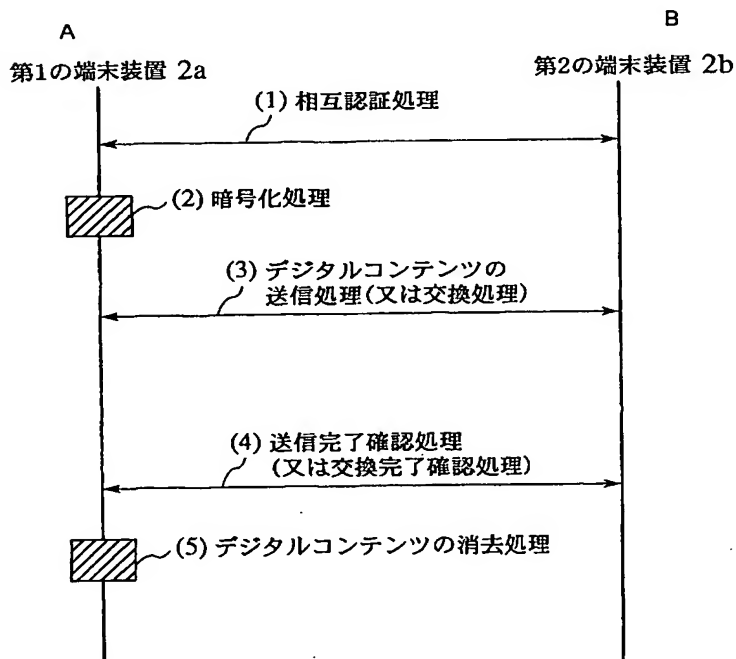
(75) 発明者/出願人 (米国についてのみ): 森 謙作 (MORI, Kensaku) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 石井 一彦 (ISHII, Kazuhiko) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.)

[続葉有]

(54) Title: IC CARD, TERMINAL DEVICE, AND DATA COMMUNICATION METHOD

(54) 発明の名称: ICカード、端末装置及びデータ通信方法



A...FIRST TERMINAL DEVICE 2a

B...SECOND TERMINAL DEVICE 2b

(1)...INTERACTIVE AUTHENTICATION

(2)...ENCRYPTION

(3)...DIGITAL CONTENT TRANSMISSION (OR EXCHANGE)

(4)...TRANSMISSION COMPLETION CONFIRMATION (OR EXCHANGE COMPLETION CONFIRMATION)

(5)...DIGITAL CONTENT ERASE

(57) Abstract: A data communication method includes a step of executing a predetermined command when an IC card (1a) has received a predetermined trigger signal, a step of storing the state of the IC card (1a) before transmitting a first digital content, a step of encrypting the first digital content according to key information related to the first digital content, a step of erasing the first digital content from a holder section (18) of the IC card (1a) when a commit instruction to notify that reception of the first digital content encrypted is complete is received from a transmission destination device (1b), and a step of returning to the state of the IC card (1a) when the transmission of the first digital content is interrupted.

[続葉有]



式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 青野 博 (AONO, Hiroshi) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 本郷 節之 (HONGO, Sadayuki) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, GB).

添付公開書類:
— 国際調査報告書

(74) 代理人: 三好 秀和 (MIYOSHI, Hidekazu); 〒105-0001 東京都港区虎ノ門1丁目2番3号 虎ノ門第一ビル9階 Tokyo (JP).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

本発明に係るデータ通信方法は、ICカード1aが所定のトリガー信号を受信すると所定のコマンドを実行する工程と、第1のデジタルコンテンツの送信前におけるICカード1aの状態を記憶する工程と、第1のデジタルコンテンツに対応付けられた鍵情報に基づいて第1のデジタルコンテンツの暗号化処理を行う工程と、暗号化された第1のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を送信先装置1bから受信した場合にICカード1aのホルダー部18から第1のデジタルコンテンツを消去する工程と、第1のデジタルコンテンツの送信処理が中断された場合にICカード1aの状態への復帰処理を行う工程とを有する。

明 細 書

I Cカード、端末装置及びデータ通信方法

5 技術分野

本発明は、電子商取引（e コマース）やコンテンツ配信等に利用可能な I Cカード、当該 I Cカードを操作するための端末装置、及び、これらを用いたデータ通信方法に関する。

10 背景技術

従来、I Cカード内に電子マネー等のデジタルコンテンツが格納されており、リーダライタ等の操作端末装置（送信元装置）が、I Cカードから当該デジタルコンテンツを読み出し、読み出したデジタルコンテンツを送信先装置に対して送信する通信プラットフォームが開発されている。

- 15 また、I Cカード内に第 1 のデジタルコンテンツが格納されており、リーダライタ等の操作端末装置（送信元装置）が、I Cカードから第 1 のデジタルコンテンツを読み出し、読み出した第 1 のデジタルコンテンツを送信先装置に対して送信するとともに、送信先装置に格納されている第 2 のデジタルコンテンツを受信することによって、デジタルコンテ
20 ンツの交換を行う通信プラットフォームが開発されている。

従来の通信プラットフォームでは、操作端末装置（送信元装置）が、I Cカードからデジタルコンテンツを読み出し、当該操作端末装置に備えられたハードウェアやソフトウェアのコマンドを用いて、当該デジタル
25 コンテンツに対する暗号化処理を行うとともに、当該操作端末装置上で実行されている O S のプロトコルに基づいて、当該デジタルコンテンツ

の送信を行っている。

かかるデジタルコンテンツの送信にあつては、当該デジタルコンテンツの安全な送信を担保するために、送信先装置に一時的に当該デジタルコンテンツを複製した後に、当該操作端末装置において当該デジタルコンテンツを消去する方式を採用している。

しかしながら、従来の通信プラットフォームでは、ＩＣカード内に格納されているデジタルコンテンツが、操作端末装置（送信元装置）上に読み出された後、当該操作端末装置のコマンドやプロトコル等により処理されるため、当該デジタルコンテンツが当該操作端末装置に読み出された際に、悪意の操作者や悪意の第三者によって当該デジタルコンテンツの内容が、改ざんされたり不正に複製されたりする可能性があった。

また、従来の通信プラットフォームでは、複数の操作端末装置間で、デジタルコンテンツの送受信処理を行う場合、当該デジタルコンテンツが送信先の操作端末装置に一時的に複製された後に、送信元の操作端末装置においてデジタルコンテンツを消去する方式を採用している。

そのため、当該デジタルコンテンツの送受信処理中に通信が切断されたときには、送信先の操作端末装置及び送信元の操作端末装置の両方において、当該送受信処理に係るデジタルコンテンツが消失してしまう可能性がある。

また、送信先の操作端末装置及び送信元の操作端末装置の両方において当該デジタルコンテンツが存在する状態で、当該デジタルコンテンツの送受信処理が中断される場合、操作者の意図によらず、当該デジタルコンテンツが送信先の操作端末装置において複製される結果となる。

特に、電子マネー等による電子商取引においては、送信元の操作端末装置と送信先の操作端末装置との間で、デジタルコンテンツが確実に交

換されるか、或いは、通信障害が生じた場合には、当該電子商取引の開始時の状態に、送信元の操作端末装置及び送信先の操作端末装置を完全に復帰させる必要がある。

5 発明の開示

そこで、本発明は、上記に鑑みてなされたものであり、ＩＣカード間で直接通信を行う通信プラットフォーム上で、デジタルコンテンツを送信する際に、送受信者及び悪意の操作者又は第三者によるデジタルコンテンツの複製や紛失を回避することのできるＩＣカード、端末装置及びデータ通信方法を提供することを目的とする。

また、本発明は、ＩＣカードと端末装置と間で直接通信を行う通信プラットフォーム上で、デジタルコンテンツを交換する際に、送受信者及び悪意の操作者又は第三者による当該デジタルコンテンツの複製や紛失を回避することのできるＩＣカード、端末装置及びデータ通信方法を提供することを目的とする。

上記目的を達成するために、本発明の第１の特徴は、ＩＣカードであって、第１のデジタルコンテンツを格納するホルダー部と、第１のデジタルコンテンツに対応付けられた鍵情報を含む証明書データを格納する証明書データ格納部と、暗号処理部と、実行処理部とを備え、実行処理部が、所定のトリガー信号を受信すると、所定のコマンドを実行し、実行処理部によって実行された所定のコマンドは、実行処理部に、第１のデジタルコンテンツの送信前におけるＩＣカードの状態を記憶させ、暗号化処理部に、第１のデジタルコンテンツに対応付けられた鍵情報に基づいて第１のデジタルコンテンツの暗号化処理を行わせ、暗号化された第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット

命令を送信先装置から受信した場合にホルダー部から第 1 のデジタルコンテンツを消去し、第 1 のデジタルコンテンツの送信処理が中断された場合に実行処理部に記憶されている IC カードの状態への復帰処理を行うことを要旨とする。

5 本発明の第 1 の特徴において、実行処理部によって実行された所定のコマンドが、コミット命令を受信した場合に送信先装置に対して第 2 のデジタルコンテンツの送信要求を送信し、第 2 のデジタルコンテンツの受信処理が完了した場合にホルダー部から第 1 のデジタルコンテンツを消去することが好ましい。

10 また、本発明の第 1 の特徴において、第 1 のデジタルコンテンツの送信に先だって、送信先装置から送信先装置の証明書データを取得し、送信先装置の証明書データに基づいて送信先装置の正当性を認証する認証部を具備し、実行処理部が、送信先装置の正当性が認証された場合に所定のコマンドを実行することが好ましい。

15 また、本発明の第 1 の特徴において、認証部が、送信先装置との間のセッションを識別するセッション ID とセッションモードとに応じて、ホルダー部に格納されている第 1 のデジタルコンテンツへのアクセスレベルを設定することが好ましい。

20 また、本発明の第 1 の特徴において、認証部が、第 1 のデジタルコンテンツの送信に先だって、証明書データ格納部に格納されている証明書データを送信先装置に対して送信し、送信先装置から証明書データの正当性が認証された旨を通知する認証確認通知を取得し、実行処理部が、認証確認通知が取得された場合に所定のコマンドを実行することが好ましい。

25 本発明の第 2 の特徴は、IC カードに格納されている第 1 のデジタル

コンテンツを送信先装置に送信する端末装置であって、入力された操作信号に基づいて所定のトリガー信号をＩＣカードに対して出力する制御部を具備し、ＩＣカードの実行処理部が、所定のトリガー信号に応じて所定のコマンドを実行し、実行処理部によって実行された前記所定のコマンドが、実行処理部に、第１のデジタルコンテンツの送信前における
5 ＩＣカードの状態を記憶させ、ＩＣカードの暗号化処理部に、第１のデジタルコンテンツに対応付けられた鍵情報に基づいて第１のデジタルコンテンツの暗号化処理を行わせ、暗号化された第１のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を送信先装置から受信した場合にＩＣカードのホルダー部から第１のデジタルコンテンツを
10 消去し、第１のデジタルコンテンツの送信処理が中断された場合に実行処理部に記憶されているＩＣカードの状態への復帰処理を行うことを要旨とする。

本発明の第２の特徴において、実行処理部によって実行された所定の
15 コマンドが、コミット命令を受信した場合に送信先装置に対して第２のデジタルコンテンツの送信要求を送信し、第２のデジタルコンテンツの受信処理が完了した場合にホルダー部から第１のデジタルコンテンツを消去することが好ましい。

また、本発明の第２の特徴において、ＩＣカードから送信先装置に第
20 １のデジタルコンテンツを送信した後、所定の待機時間を経過するまでの間に送信先装置から応答がない場合、第１のデジタルコンテンツの送信処理が中断された旨をＩＣカードに通知する通信監視部を具備することが好ましい。

また、本発明の第２の特徴において、ＩＣカードと送信先装置との間
25 で確立されているセッションを識別するセッションＩＤとセッションモ

ードとに応じて設定されたアクセスレベルに基づいて、ホルダー部から第1のデジタルコンテンツに関する情報を読み出して表示する表示部を具備することが好ましい。

本発明の第3の特徴は、ICカードに格納されている第1のデジタルコンテンツを送信先装置に送信するデータ通信方法であって、ICカードが、所定のトリガー信号を受信すると、所定のコマンドを実行する工程と、第1のデジタルコンテンツの送信前におけるICカードの状態を記憶する工程と、第1のデジタルコンテンツに対応付けられた鍵情報に基づいて第1のデジタルコンテンツの暗号化処理を行う工程と、暗号化された第1のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を送信先装置から受信した場合にICカードのホルダー部から第1のデジタルコンテンツを消去する工程と、第1のデジタルコンテンツの送信処理が中断された場合に、記憶されているICカードの状態への復帰処理を行う工程とを有することを要旨とする。

また、本発明の第3の特徴において、コミット命令を受信した場合、送信先装置に対して第2のデジタルコンテンツの送信要求を送信する工程と、第2のデジタルコンテンツの受信処理が完了した場合、ホルダー部から第1のデジタルコンテンツを消去する工程とを有することが好ましい。

また、本発明の第3の特徴において、ICカードが装填された端末装置が、入力された操作信号に基づいて、所定のトリガー信号を、ICカードに対して出力する工程を有することが好ましい。

また、本発明の第3の特徴において、第1のデジタルコンテンツの送信に先だって、送信先装置から送信先装置の証明書データを取得する工程と、送信先装置の証明書データに基づいて送信先装置の正当性を認証

する工程と、ＩＣカードが、送信先装置の正当性が認証された場合に所定のコマンドを実行する工程とを有することが好ましい。

また、本発明の第３の特徴において、送信先装置との間のセッションを識別するセッションＩＤとセッションモードとに応じて、ホルダー部に格納されている第１のデジタルコンテンツへのアクセスレベルを設定
5 する工程を有することが好ましい。

また、本発明の第３の特徴において、第１のデジタルコンテンツの送信に先だって、証明書データ格納部に格納されている証明書データを送信先装置に対して送信する工程と、送信先装置から証明書データの正当
10 性が認証された旨を通知する認証確認通知を取得する工程と、ＩＣカードが、認証確認通知が取得された場合に所定のコマンドを実行する工程とを有することが好ましい。

また、本発明の第３の特徴において、ＩＣカードから送信先装置に第１のデジタルコンテンツを送信した後、所定の待機時間を経過するまで
15 の間に送信先装置から応答がない場合、第１のデジタルコンテンツの送信処理が中断された旨をＩＣカードに通知する工程を有することが好ましい。

また、本発明の第３の特徴において、端末装置が、ＩＣカードと送信先装置との間で確立されているセッションを識別するセッションＩＤと
20 セッションモードとに応じて設定されたアクセスレベルに基づいて、ホルダー部から第１のデジタルコンテンツに関する情報を読み出して表示する工程を有することが好ましい。

図面の簡単な説明

25 図１は、本発明の第１の実施形態に係るデータ通信方法を実現するシ

システムの全体構成図である。

図 2 は、本発明の第 1 の実施形態に係る端末装置及び I C カードの内部構造を示す図である。

図 3 は、本発明の第 1 の実施形態に係るデータ通信方法の全体動作を示すシーケンス図である。

図 4 は、本発明の第 1 の実施形態に係るデータ通信方法の全体動作を示すフローチャートである。

図 5 は、本発明の第 1 の実施形態に係るデータ通信方法における相互認証処理を示すフローチャートである。

10 図 6 は、本発明の第 1 の実施形態に係るデータ通信方法における第 1 の I C カード側の送信処理を示すフローチャートである。

図 7 は、本発明の第 1 の実施形態に係るデータ通信方法における第 2 の I C カード側の送信処理を示すフローチャートである。

図 8 は、本発明の第 1 の実施形態に係るデータ通信方法における交換
15 処理を示すフローチャートである。

図 9 は、本発明の第 1 の実施形態に係るデータ通信方法における通信状況の監視処理を示すフローチャートである。

図 1 0 は、本発明の第 2 の実施形態に係るデジタルコンテンツ発行システムの概略構成図である。

20 図 1 1 は、本発明の第 2 の実施形態に係るデジタルコンテンツ発行システムの概略構成図である。

図 1 2 は、本発明の第 2 の実施形態に係るデジタルコンテンツ発行システムの概略構成図である。

図 1 3 は、本発明の第 2 の実施形態に係るデジタルコンテンツ発行シ
25 ステムの動作を示すシーケンス図である。

図 1 4 は、本発明の変更例 1 に係るデジタルコンテンツ発行システムの概略構成図である。

図 1 5 は、本発明の変更例 1 に係るデジタルコンテンツ発行システムの概略構成図である。

- 5 図 1 6 は、本発明の変更例 1 に係るデジタルコンテンツ発行システムの動作を示すシーケンス図である。

図 1 7 は、本発明の変更例 2 に係るデジタルコンテンツ発行システムの概略構成図である。

- 10 図 1 8 は、本発明の変更例 2 に係るデジタルコンテンツ発行システムの概略構成図である。

図 1 9 は、本発明の変更例 3 に係るデジタルコンテンツ発行システムの概略構成図である。

図 2 0 は、本発明の変更例 3 に係るデジタルコンテンツ発行システムの概略構成図である。

- 15 図 2 1 は、本発明の変更例 3 に係るデジタルコンテンツ発行システムの動作を示すシーケンス図である。

発明を実施するための最良の形態

[第 1 の実施形態]

- 20 本発明の第 1 の実施形態に係るデータ通信方法、当該データ通信方法に用いて好適な I C カード及び端末装置について、図を参照しながら説明する。

図 1 は、本実施形態に係るデータ通信方法を実現するためのシステムの構成を示す説明図である。

- 25 図 1 に示すように、本実施形態では、機能分散システム上において、

「送信元装置」である第１のＩＣカード１ａに格納されている「第１のデジタルコンテンツ」を、「送信先装置」である第２のＩＣカード１ｂに対して送信し、第２のＩＣカード１ｂに格納されている「第２のデジタルコンテンツ」を、第１のＩＣカード１ａに送信する場合を例に説明する。

図１に示すように、第１のＩＣカード１ａ及び第２のＩＣカード１ｂは、それぞれ、第１のＩＣチップ１１ａ及び第２のＩＣチップ１１ｂを搭載している。具体的には、第１のＩＣチップ１１ａ及び第２のＩＣチップ１１ｂは、プラスチック等で形成された第１のＩＣカード１ａ及び第２のＩＣカード１ｂの基板上に固着された集積回路である。

また、第１のＩＣカード１ａ及び第２のＩＣカード１ｂは、それぞれ第１の端末装置２ａ及び第２の端末装置２ｂに装填されており、各端末装置２ａ及び２ｂからの操作に基づいて、当該端末装置２ａ及び２ｂを介して、第１及び第２のデジタルコンテンツの送受信処理を行う。

図２は、第１のＩＣカード１ａ（又は、第２のＩＣカード１ｂ）及び第１の端末装置２ａ（又は、第２の端末装置２ｂ）の内部構成を示すブロック図である。

第１のＩＣカード１ａの内部構成及び第２のＩＣカード１ｂの構成は基本的に同一であり、第１の端末装置２ａの内部構成及び第２の端末装置２ｂの内部構成も、基本的に同一であるため、以下、第１のＩＣカード１ａ及び第１の端末装置２ａの内部構成について説明する。

図２に示すように、第１のＩＣカード１ａは、第１のＩＣチップ１１ａと第１の端末装置２ａとの間で、例えば、デジタルコンテンツや証明書データやコミット命令（後述）や送信要求（後述）等のデータの送受信処理を行うデータ送受信部１２を備えている。

本実施形態において、第1のICカード1aは、コンピュータの周辺機器として、リーダライタ等の操作端末装置を通して操作されるものではなく、分散環境におけるノードとして設計されており、ネットワーク上のサービス提供モジュールのチップに対して、対等に「Peer-to-Peer」で通信が可能となっている。

第1のICチップ11aは、耐タンパ性を有するLSIであり、演算処理デバイスやメモリ等から構成されており、ICカードの他、例えば、スマートカードやPDA端末といったハードウェア上に実装されることも可能である。

第1の端末装置2aには、第1のICカード1aが、挿抜可能に装填されている。また、第1の端末装置2aは、第1のICカード1aとの間で、データの読込処理及び書込処理を行うリーダライタ機能を備えており、LAN等の通信ネットワークに対する非接触（コンタクトレス）通信の物理層を橋渡しするゲートウェイ（ブリッジ）の役割を果たすものである。

具体的に、第1の端末装置2aは、例えば、PDA端末や携帯電話端末等の形態を採ることができる。

（本実施形態に係るICカード）

本実施形態に係る第1のICカード1aは、図2に示すように、認証部13と、暗号処理部14と、実行処理部15と、コマンド記憶部16と、証明書データ格納部17と、ホルダー部18とを備えている。

認証部13は、他のICカード（例えば、第2のICカード1b）との通信を確立する際に、当該他のICカードとの間で相互認証処理を行う演算デバイスである。

具体的には、認証部13は、第1のデジタルコンテンツの送信に先だ

って、第2のICカード1bから当該第2のICカード1bの証明書データを取得し、取得した証明書データに含まれる当該第2のICカード1bのホルダーIDと署名データとに基づいて、当該第2のICカード1bの正当性を認証するとともに、当該第2のICカード1bに対して
5 当該第1のICカード1aの証明書データを送信し、当該第2のICカード1bから、当該第1のICカード1aの証明書データの正当性が認証された旨を通知する「認証確認通知」を取得することによって、当該第2のICカード1bとの間で相互認証処理を行う。

また、本実施形態において、認証部13は、第2のICカード1bとの間の相互認証処理の際に、当該第2のICカード1bとの間で確立されている通信（セッション）を識別する「セッションID」と、指定された「セッションモード」とを取得し、取得された「セッションID」と「セッションモード」とに応じて、ホルダー部18に格納されているデジタルコンテンツへのアクセスレベルを設定する。
10

本実施形態では、当該セッションモードには、以下に示すように、「（情報）発行者モード」と「所有者モード」の2つのモードがある。これらのセッションモードは、第1のICカード1aと第2のICカード1bとの間の相互認証処理時に指定されるものである。各セッションモードによって、用いられる認証アルゴリズムが異なる。
15

「（情報）発行者モード」は、アクセス者（例えば、第2のICカード1b）を、当該デジタルコンテンツの発行者として認証するセッションモードである。
20

「（情報）発行者モード」による認証によって設定されたアクセスレベルを有するアクセス者は、当該情報発行者が作成したデジタルコンテンツには、発行者権限でアクセスでき、それ以外のデジタルコンテンツ
25

には、その他権限でアクセスすることができる。

「所有者モード」は、アクセス者（例えば、第2のICカード1b）を第1のICカード1aの所有者として認証するモードである。本実施形態において、「所有者モード」による認証では、パスワード等、人間
5 にとって扱いやすい認証方法が使用される。

「所有者モード」による認証によって設定されたアクセルレベルを有するアクセス者は、所有者権限を持つ。

暗号処理部14は、第1のICカード1a内部において、ホルダー部18に格納されている第1のデジタルコンテンツについての暗号化処理
10 を行うものである。ホルダー部18に格納されている第1のデジタルコンテンツは、暗号処理部14によって暗号化処理が施された後、データ送受信部12を通じて、第1の端末装置2a側に送出される。

実行処理部15は、外部からの所定のトリガー信号に基づいて、コマンド記憶部16から所定のコマンドを呼び出し、第1のデジタルコンテンツの暗号化処理や送信処理を実行する演算処理装置である。本実施形
15 態において、所定のトリガー信号は、操作部24からの操作信号に基づいて、制御部26によって出力されるものである。

また、実行処理部15は、認証部13と連動する形態となっており、認証部13が、第2のICカード1bが正当であると認証するとともに、
20 当該第2のICカード1bから認証確認通知を取得して、当該第2のICカード1bとの間の相互認証処理が完了された場合に、上述の所定のコマンドを実行する。

コマンド記憶部16は、所定のコマンドを記憶するメモリ等の記憶装置である。

25 例えば、所定のコマンドは、暗号処理部14に対して、ホルダー部1

8に格納されている第1のデジタルコンテンツを暗号化させたり、データ送受信部12に対して、第2のICカードIC1bに第1のデジタルコンテンツを送信させたり、第2のICカードIC1bから第2のデジタルコンテンツを受信させたりするためのコマンドである。

- 5 証明書データ格納部17は、ホルダー部18に格納されている第1のデジタルコンテンツに対応付けられた証明書データ（後述）を格納するメモリ等の記憶装置である。証明書データ格納部17は、認証部13による認証処理や暗号処理部14による暗号化処理の際に、これらの処理に必要なデータである「ホルダーID」や「鍵情報」や「署名データ」
- 10 を提供するものである。

ホルダー部18は、他のICカード（例えば、第2のICカード1b）等との間で情報交換を行うネットワーク上の計算実体であり、第1のデジタルコンテンツを格納する耐タンパ性のメモリ装置である。

- データ送受信部12は、接触式通信或いは非接触式通信によって、暗
- 15 号化された第1のデジタルコンテンツや、第1のICカード1aの証明書データや等の各種データを、外部に対して送信する通信デバイスである。

- なお、本実施形態におけるデータ送受信部12は、第1のICカード
- 1 aが第1の端末装置2a内に装填された状態において、当該第1の端
- 20 末装置2a側のデータ送受信部23と接触して、各種データの送受信処理を行うように形成されている。

（本実施形態に係る端末装置）

- 本実施形態に係る第1の端末装置2aは、カードリーダーや携帯電話端
- 末やPDA端末等の携帯端末装置、或いはパーソナルコンピュータ等の
- 25 汎用コンピュータで実現することが可能である。

図 2 に示すように、第 1 の端末装置 2 a は、通信部 2 1 と、通信監視部 2 2 と、データ送受信部 2 3 と、操作部 2 4 と、表示部 2 5 と、制御部 2 6 とを備えている。

通信部 2 1 は、無線通信等によって、外部（例えば、第 2 の端末装置 5 2 b）との間で各種データの送受信を行う通信デバイスである。

通信監視部 2 2 は、通信部 2 1 による通信状態を監視する装置である。また、通信監視部 2 2 は、最後にデータを送信した時点からの経過時間を測定し、所定の待機時間を経過するまでの間に送信先からの応答がない場合に、通信が中断されたと判断し、その旨をデータ送受信部 2 3 及び 1 2 を介して、第 1 の IC カード 1 a 内の実行処理部 1 5 に送出する。

データ送受信部 2 3 は、第 1 の端末装置 2 a 内に装填された第 1 の IC カード 1 a のデータ送受信部 1 2 と接触されるように設けられており、データ送受信部 1 2 との間で各種データの送受信処理を行うものである。

操作部 2 4 は、例えば、第 1 の端末装置 2 a の表面に配置されたボタンやスティックであり、操作者の操作により、種々の操作信号を制御部 15 2 6 に対して入力する操作デバイスである。

表示部 2 5 は、例えば、第 1 の端末装置 2 a の表面に配置された液晶ディスプレイ等の表示デバイスであり、通信部 2 1 による通信状態や、操作部 2 4 による操作結果を表示する。

20 特に、本実施形態において、表示部 2 5 は、現在、第 1 の IC カード 1 a と他の IC カード（例えば、第 2 の IC カード 1 b）との間で確立されている通信（セッション）を識別する「セッション ID」と、指定された「セッションモード」とに応じて設定されたアクセスレベルに基づいて、当該デジタルコンテンツに関する情報をホルダー部 1 8 から読
25 み出して表示する機能を有する。

制御部 26 は、第 1 の端末装置 2 a における各部 21 乃至 25 の動作を制御する CPU である。特に、制御部 26 は、操作部 24 からの操作信号に基づいて、実行処理部 15 に対して、所定のコマンドの実行処理を開始させるトリガー信号を出力する。

5 (デジタルコンテンツ)

第 1 の IC カード 1 a には、第 1 のデジタルコンテンツを格納する多様なアプリケーションが実装される可能性があるため、第 1 のデジタルコンテンツとしては、様々なタイプが想定される。

例えば、第 1 のデジタルコンテンツとして、以下のようなものが考えられる。

- ・ 第 1 の IC カード 1 a の所有者が変更することができず、情報発行者だけが変更することができるデジタルコンテンツ（例えば、電子チケットの座席番号）
- ・ 第 1 の IC カード 1 a の所有者でさえ見ることができないデジタルコンテンツ（例えば、電子チケットを変更するための鍵情報）
- ・ 第 1 の IC カード 1 a の所有者だけが完全に制御できるデジタルコンテンツ（例えば、第 1 の IC カード 1 a の所有者の個人情報）
- ・ 何人も読むことができるデジタルコンテンツ

なお、これらの第 1 のデジタルコンテンツは、発行サーバ等の第三者機関により発行され、証明書データとともに第 1 の IC カード 1 a 内に格納される。

(証明書データ)

証明書データには、ホルダー部 18 に格納されている第 1 のデジタルコンテンツを識別する「ホルダー ID」と、証明書データを発行した者が当該証明書データが正当である旨を保証する「署名データ」と、当該

第 1 のデジタルコンテンツに関連付けられた「公開鍵（鍵情報）」が含まれている。

「ホルダー ID」は、分散システム（分散環境）全体でユニークに定められた識別子であり、第 1 の IC カード 1 a を物理的に識別するだけでなく、分散システム上での経路制御にも利用され、認証通信における
5 相手に対する識別子としても利用される。すなわち、「ホルダー ID」は、ネットワーク上で、IC カードやサービスクライアントの認証、メッセージの経路制御等に用いられる。なお、本実施形態において、「ホルダー ID」は、16 オクテット（128 ビット）で表現される。

10 （コマンド）

コマンド記憶部 16 に格納されている所定のコマンドは、第 1 の端末装置 2 a 側から受信した所定のトリガー信号に応じて、実行が開始されると、第 2 の端末装置 2 a 側における操作とは独立してアトミックに一連の処理が進行される原子性を有するものである。

15 当該所定のコマンドによる一連の処理としては、

（1）相互認証処理

（2）暗号化処理

（3）デジタルコンテンツの送信処理又は交換処理

（4）送信完了確認処理又は交換完了確認処理

20 （5）デジタルコンテンツの消去処理

がある。

ここで、所定のコマンドは、実行処理部 15 に対して、デジタルコンテンツの送信処理（又は、交換処理）に先立って、第 1 の IC カード 1 a 内における「各部 12 乃至 19 の状態（IC カードの状態）」を記憶

25 させる。

また、所定のコマンドは、当該第 1 のデジタルコンテンツの送信処理完了後、データ送受信部 12 を介して、第 2 の IC カード 1b から「受信処理を完了した旨」を通知する「コミット命令」を受信した場合に、ホルダー部 18 内に格納されている当該第 1 のデジタルコンテンツを消去する。

また、所定のコマンドは、第 2 の IC カード 1b から受信した「コミット命令」に応じて、第 2 の IC カード 1b に対して第 2 のデジタルコンテンツの「送信要求」を送信し、当該「送信要求」に応じて第 2 の IC カード 1b から送信された第 2 のデジタルコンテンツの受信処理が完了した場合に、その旨を通知する「送信完了要求」を送信すると共に、ホルダー部 18 内に格納されている当該第 1 のデジタルコンテンツを消去するように構成されていても良い。

また、所定のコマンドは、当該第 1 のデジタルコンテンツの送信処理（又は、デジタルコンテンツの交換処理）の実行中に、通信が中断された場合には、実行処理部 15 に記憶されている「各部 12 乃至 19 の状態（IC カードの状態）」を読み出し、ロールバック処理（復帰処理）によって、第 1 の IC カード 1a 内の各部 12 乃至 19 を、当該デジタルコンテンツの送信処理（又は、交換処理）開始前の状態（読み出した「各部 12 乃至 19 の状態（IC カードの状態）」）に復帰させる。

また、所定のコマンドは、第 2 の IC カード 1b の実行処理部 15 に対して、当該デジタルコンテンツの送信処理（又は、交換処理）開始前における第 2 の IC カード 1b 内の「各部 12 乃至 19 の状態（IC カードの状態）」を記憶させ、当該デジタルコンテンツの送信処理（又は、交換処理）が中断された場合に、第 2 の IC カード 1b 内の各部 12 乃至 19 を、第 2 の IC カード 1b の実行処理部 15 に記憶されている「各

部 1 2 乃至 1 9 の状態（ＩＣカードの状態）」に復帰させる。

（本実施形態に係るデータ通信方法）

図を参照して、本実施形態に係るデータ通信方法について説明する。

ここで、図 3 乃至図 9 は、本実施形態に係るデータ通信方法の手順を示すフロー図である。なお、本実施形態では、第 1 の ＩＣカード 1 a の操作者による操作に基づいて、第 1 の ＩＣカード 1 a から第 2 の ＩＣカード 1 b への第 1 のデジタルコンテンツの送信処理、及び、第 1 の ＩＣカード 1 a と第 2 の ＩＣカード 1 b との間で行われる第 1 及び第 2 のデジタルコンテンツの交換処理の双方に係るデータ通信方法について説明する。

（１） 全体処理

図 3 を参照して、本実施形態に係るデータ通信方法の全体処理について説明する。

図 3 に示すように、本実施形態に係るデータ通信方法では、ステップ（１）において、第 1 の端末装置 2 a と第 2 の端末装置 2 b との間で、相互認証処理が行われる。ステップ（２）において、相互認証処理及びが完了した後に、デジタルコンテンツについての暗号化処理が行われる。ステップ（３）において、暗号化処理が完了した後に、デジタルコンテンツの送信処理（又は、交換処理）が行われる。ステップ（４）において、第 1 及び第 2 の端末装置 2 a、2 b において、デジタルコンテンツの送信完了確認処理及び交換完了確認処理が行われる。ステップ（５）において、デジタルコンテンツの消去処理が行われる。

このとき、前提として、第 1 の ＩＣカード 1 a 内には、既に第 1 のデジタルコンテンツが格納されているものとする。

すなわち、図 4 に示すように、第 1 のデジタルコンテンツの情報発行

者が、ステップS 1 0 1において、第1のデジタルコンテンツ及び証明書データを発行する。

第1のICカード1 aから第2のICカード1 bへの第1のデジタルコンテンツの送信処理の場合、ステップS 1 0 2において、第1のデジタルコンテンツの情報発行者が、当該第1のデジタルコンテンツ及び当該証明書データを、それぞれ第1のICカード1 a内のホルダー部1 8及び証明書データ格納部1 7に格納する。

また、第1のICカード1 aと第2のICカード1 bとの間で行われる第1及び第2のデジタルコンテンツの交換処理の場合、ステップS 1 0 2において、第1及び第2のデジタルコンテンツの情報発行者は、当該第1及び第2のデジタルコンテンツ及び当該証明書データを、それぞれ、第1のICカード1 a及び第2のICカード1 b内のホルダー部1 8及び証明書データ格納部1 7に格納する。

ここで、証明書データには、当該証明書データの格納先である第1のICカード1 a又は第2のICカード1 bを識別する「ホルダーID」と、ホルダー部1 8に格納されている第1又は第2のデジタルコンテンツに対応付けられた「公開鍵（鍵情報）」と、当該情報発行者によって当該第1又は第2のデジタルコンテンツが正当である旨を証明するための「署名データ」とが含まれている。

ステップS 1 0 3において、第1の端末装置2 aの操作者が、当該デジタルコンテンツの送信処理（又は、交換処理）を行うための操作を開始する。具体的には、第1の端末装置2 aの操作者が、第1の端末装置2 aの操作部2 4において、デジタルコンテンツの送信処理（又は、交換処理）を開始するための操作を行い、この操作に応じて、制御部2 6は、データ送受信部2 3及び1 2を通じて、第1のICカード1 aに所

定のトリガー信号を出力する。

第1のICカード1aの実行処理部15は、当該所定のトリガー信号に応じて、コマンド記憶部16から所定のコマンドを読み出して、読み出した所定のコマンドを実行する。

- 5 その結果、ステップS104において、認証部13が、第2のICカード1bとの間の相互認証処理を行い、ステップS105において、第1のICカード1aの暗号処理部14が、第1のデジタルコンテンツの暗号化処理を行い、ステップS106において、第1の端末装置2aの通信部21が、第2のICカード1bとの間で第1のデジタルコンテンツの送信処理（又は、第1及び第2のデジタルコンテンツの交換処理）
10 を開始する。

- 当該デジタルコンテンツの送信処理（又は、交換処理）の間、通信監視部22は、ステップS107において、第1のICカード1aと第2のICカード1bとの間の通信状態を監視しており、ステップS108
15 において、当該デジタルコンテンツの送信処理（又は、交換処理）が中断されないか否かについて判断する。

- 当該デジタルコンテンツの送信処理（又は、交換処理）が中断されなかった場合、すなわち、当該デジタルコンテンツの送信処理（又は、交換処理）が正常に完了した場合、ステップS109において、送信完了
20 確認処理（又は、交換完了確認処理）が行われ、第1のICカード1a（及び、第2のICカード1b）のホルダー部18内の第1のデジタルコンテンツの消去処理が行われる。

- 一方、当該デジタルコンテンツの送信処理（又は、交換処理）が中断された場合、すなわち、当該デジタルコンテンツの送信処理（又は、交換処理）が正常に完了しなかった場合は、ステップS110において、
25

復帰処理が行われる。

(2) 相互認証処理

以下、図5を参照して、上述のステップS104における相互認証処理について詳細に説明する。図5は、本実施形態に係るデータ通信方法
5 における相互認証処理の動作を示すフロー図である。

図5に示すように、第1の端末装置2aにおいて、相互認証処理が開始されると、ステップS201において、第1のICカード1aの認証部13が、証明書データ格納部17に格納されている証明書データを、第1の端末装置2aの通信部21を介して、第2の端末装置2b内の第
10 2のICカード1bに送信する。

ステップS202において、第2のICカード1bの認証部13は、受信した証明書データに含まれる「署名データ」と「ホルダーID」とに基づいて、第1のICカード1aの正当性についての認証処理を行う。

第1のICカード1aの正当性が確認された場合には、ステップS2
15 03において、第2のICカード1bの認証部13は、その旨を示す「認証確認通知」を、第1のICカード1aに対して送信する。一方、第1のICカード1aの正当性が否認された場合には、当該相互認証処理は中断される。

ステップS204において、第1のICカード1aの認証部13が、
20 第2のICカード1bから送信された「認証確認通知」を受信した場合、第2のICカード1bにおける認証処理は、終了する。

このような第2のICカード1bにおける認証処理と並行して、第1のICカード1aにおいても同様な認証処理が実行される。

すなわち、ステップS205において、第1のICカード1aの認証
25 部13は、第2のICカード1bから証明書データを取得する。ステッ

プ S 2 0 6 において、第 1 の I C カード 1 a の認証部 1 3 は、取得した証明書データに含まれる「署名データ」と「ホルダー I D」とに基づいて、第 2 の I C カード 1 b の正当性についての認証処理を行う。

第 1 の I C カード 1 a 及び第 2 の I C カード 1 b の認証部 1 3 は、ス
5 テップ S 2 0 7 において、当該セッションでのみ有効な「セッション I D」を設定するとともに、セッションモードを相互に取得しあう。

ステップ S 2 0 8 において、第 1 の I C カード 1 a の認証部 1 3 は、取得したセッションモードと、第 2 の I C カード 1 b のカード I D（ホルダー I D）とに基づいて、当該デジタルコンテンツに対するアクセス
10 レベルを設定する。

設定されたアクセスレベルに応じて、ホルダー部 1 8 内のデジタルコンテンツのセキュリティーレベルが決定されると共に、操作者に開示するデジタルコンテンツの内容が制限される。ここで、開示を制限されていないデジタルコンテンツは、ホルダー部 1 8 から読み出されることが
15 可能であり、表示部 2 5 に表示される。また、表示されるデジタルコンテンツとしては、デジタルコンテンツのファイル名や、デジタルコンテンツの種類（電子マネーやクーポン・チケット等）等が考えられる。

上述のように、相互認証処理が完了した後、第 1 の I C カード 1 a の実行処理部 1 5 は、コマンド記憶部 1 6 に記憶されている所定のコマン
20 ドを呼び出し、デジタルコンテンツの送信処理（又は、交換処理）を実行する。

（3-1） 送信処理

以下、図 6 及び図 7 を参照して、上述のステップ S 1 0 6 における送信処理について詳細に説明する。図 6 は、本実施形態に係るデータ通信
25 方法における第 1 の I C カード 1 a 側の送信処理の動作を示すフロー図

であり、図 7 は、本実施形態に係るデータ通信方法における第 2 の I C
カード 1 a b の送信処理の動作を示すフロー図である。

図 6 に示すように、第 1 のデジタルコンテンツの送信処理が開始され
ると、ステップ S 4 0 1 において、第 1 の I C カード 1 a の実行処理部
5 1 5 が、第 1 のデジタルコンテンツの送信処理開始時の各部 1 2 乃至 1
9 の状態 (I C カードの状態) を記憶する。ステップ S 4 0 2 において、
第 1 の I C カード 1 a のデータ送受信部 1 2 が、暗号化されている第 1
のデジタルコンテンツを、第 2 の I C カード 1 b に対して送信する。

ステップ S 4 0 3 において、第 2 の I C カード 1 b のデータ送受信部
10 1 2 が、当該第 1 のデジタルコンテンツの受信処理を完了すると、ステ
ップ S 4 0 4 において、第 2 の I C カード 1 b の実行処理部 1 5 は、当
該第 1 のデジタルコンテンツの受信処理が正常に完了した旨を通知する
「コミット命令」を、第 1 の I C カード 1 a に対して送信する。

ステップ S 4 0 5 において、第 1 の I C カード 1 a のデータ送受信部
15 1 2 が、当該コミット命令を受信すると、ステップ S 4 0 6 において、
第 1 の I C カード 1 a の実行処理部 1 5 は、ホルダー部 1 8 から第 1 の
デジタルコンテンツを消去する。

一方、ステップ S 4 0 5 において、第 1 の I C カード 1 a のデータ送
受信部 1 2 が、当該コミット命令を受信しない場合、ステップ S 4 0 7
20 において、第 1 の I C カード 1 a の実行処理部 1 5 は、第 1 のデジタル
コンテンツの消去処理を行わず、各部 1 2 乃至 1 9 を、記憶している送
信処理開始時の各部 1 2 乃至 1 9 の状態 (I C カードの状態) に復帰さ
せる。

図 7 に示すように、第 1 のデジタルコンテンツの送信処理が開始され
25 ると、ステップ S 3 0 1 において、第 2 の I C カード 1 b の実行処理部

15 15が、送信処理開始時の各部12乃至19の状態（ICカードの状態）を記憶する。その後、第2のICカード1bにおいて、当該第1のデジタルコンテンツの受信処理が開始されると、第2のICカード1bは、受信した第1のデジタルコンテンツの蓄積を行う。

- 5 ステップS302において、当該第1のデジタルコンテンツの送信処理が中断されることなく終了した場合は、第2のICカード1bは、受信した第1のデジタルコンテンツを保存して、当該送信処理は終了する。

一方、ステップS302において、当該第1のデジタルコンテンツの送信処理の中断が生じた場合には、ステップS303において、第2の
10 ICカード1bの実行処理部15は、各部12乃至19を、記憶している送信処理開始時の各部12乃至19の状態（ICカードの状態）に復帰させる。このとき、受信されていた第1のデジタルコンテンツは消去される。

（3-2） 交換処理

- 15 以下、図8を参照して、上述のステップS106における交換処理について詳細に説明する。図8は、本実施形態に係るデータ通信方法における交換処理の動作を示すフロー図である。

図8に示すように、交換処理が開始されると、ステップS601及びS602において、第1のICカード1a及び第2のICカード1bの
20 実行処理部15が、交換処理開始時の各部12乃至19の状態（ICカードの状態）を記憶する。

ステップS603において、第1のICカード1aのデータ送受信部12が、第1の端末装置2aの通信部21を介して、第2のICカード1bに対して、暗号化された第1のデジタルコンテンツの送信を行う。

- 25 ステップS604において、第2のICカード1bのデータ送受信部

1 2 が、当該第 1 のデジタルコンテンツの受信処理を完了すると、ステップ S 6 0 5 において、第 2 の I C カード 1 b の実行処理部 1 5 が、当該第 1 のデジタルコンテンツの受信処理が正常に完了した旨を通知する「コミット命令」を、第 1 の I C カード 1 a に対して送信する。

- 5 ステップ S 6 0 6 において、第 1 の I C カード 1 a のデータ送受信部 1 2 が、当該コミット命令を受信すると、第 1 の I C カード 1 a の実行処理部 1 5 は、第 2 の I C カード 1 b に対して、第 2 のデジタルコンテンツの「送信要求」を送信する。ステップ S 3 0 7 において、第 2 の I C カード 1 b のデータ送受信部 1 2 が、当該送信要求を受けて、第 1 の
- 10 I C カード 1 a に対して、第 2 のデジタルコンテンツの送信を行う。

第 1 の I C カード 1 a のデータ送受信部 1 2 が、当該第 2 のデジタルコンテンツの受信処理を完了すると、ステップ S 6 0 8 において、その旨を示す「コミット命令」を、第 2 の I C カード 1 b に対して送信する。

- ステップ S 6 0 9 において、第 2 の I C カード 1 b のデータ送受信部
- 15 1 2 が、当該コミット命令を受信した場合、すなわち、当該デジタルコンテンツの交換処理が中断されることなく正常に終了した場合、ステップ S 6 1 0 において、第 1 の I C カード 1 a 及び第 2 の I C カード 1 b の実行処理部 1 5 が、ホルダー部 1 8 から第 1 のデジタルコンテンツを消去する。

- 20 一方、ステップ S 6 0 6 において、第 1 の I C カード 1 a の実行処理部 1 5 は、上述のコミット命令を受信しなかった場合、ステップ S 6 1 1 において、第 2 の I C カード 1 b に対して送信処理を完了している第 1 のデジタルコンテンツを消去することなく、各部 1 2 乃至 1 9 を、記憶している交換処理開始時の各部 1 2 乃至 1 9 の状態（I C カードの状態）
- 25 に復帰させる。

かかる場合、第2のICカード1bの実行処理部15は、第1のICカード1aから送られてきて一時的に保持している第1のデジタルコンテンツを消去すると共に、各部12乃至19を、記憶している交換処理開始時の各部12乃至19の状態（ICカードの状態）に復帰させる。

5 また、ステップS609において、第2のICカード1aの実行処理部15が、上述のコミット命令を受信しなかった場合、ステップS611において、第1のICカード1aの実行処理部15は、第2のICカード1bから送られてきて一時的に保持している第2のデジタルコンテンツを消去する。また、第1のICカード1aの実行処理部15は、第
10 2のICカード1bに対して送信処理を完了している第1のデジタルコンテンツを消去することなく、各部12乃至19を、記憶している交換処理開始時の各部12乃至19の状態（ICカードの状態）に復帰させる。

かかる場合、第2のICカード1aの実行処理部15は、第1のIC
15 カード1aに対して送信を完了している第2のデジタルコンテンツを消去することなく、各部12乃至19を、記憶している交換処理開始時の各部12乃至19の状態（ICカードの状態）に復帰させる。また、第2のICカード1aの実行処理部15は、第1のICカード1aから送られてきて一時的に保持している第1のデジタルコンテンツを消去する

20 (4) 監視処理

以下、図9を参照して、上述のステップS107における通信状態の監視処理について詳細に説明する。図9は、本実施形態に係るデータ通信方法における監視処理の動作を示すフロー図である。

図9に示すように、第1のICカード1aのデータ送受信部12が、
25 暗号化された第1のデジタルコンテンツを、第2のICカード1bに対

して送信する。ステップS501において、第1のICカード1aの実行処理部15が、デジタルコンテンツの送信時刻を計測し、最後にデジタルコンテンツを送信した時点を経過時間を記憶する。

第1のICカード1aの実行処理部15が、ステップS502において、最後にデジタルコンテンツを送信した時点からの経過時間を測定し、ステップS503及びS504において、所定長の待機時間が経過する間に、第2のICカード1bから何らかの応答があるか否かを判断を行う。

ステップS504において、第2のICカード1bからの応答があった場合は、第1のICカード1aの実行処理部15は、ステップS502において、継続して経過時間の測定を行う。

一方、ステップS504において、第2のICカード1bからの応答が無かったと判断された場合には、第1のICカード1aの実行処理部15は、ステップS505において、監視処理についての中断処理を行う。この中断処理としては、上述した復帰処理（例えば、図4に示すステップS110）が考えられる。

[第2の実施形態]

(基本構成)

次いで、本発明の第2の実施形態について説明する。本実施形態では、本発明の第1の実施形態に係るデータ通信方法を、電子チケットや電子クーポンの配布等の電子商取引に応用することを特徴とする。

すなわち、本実施形態に係るデータ通信方法では、図10に示すように、上述の第1の実施形態に係る第1のICカード1aが、電子チケット等のデジタルコンテンツを発行するコンテンツ発行サーバ11に装填されて用いられる。

また、本実施形態に係るデータ通信方法では、コンテンツ発行サーバ 11 により発行されたデジタルコンテンツは、当該コンテンツ発行サーバ 11 から第 2 の IC カード 1 b に送信され、当該第 2 の IC カード 1 b は、当該コンテンツ発行サーバ 11 から送信されたデジタルコンテンツの代金として電子マネーを支払う。

図 10 乃至図 12 は、第 2 の実施形態に係るデータ通信方法を採用したデジタルコンテンツ発行システムの構成を模式的に示す説明図である。

図 10 に示すように、デジタルコンテンツ発行システムは、第 2 の IC カード 1 b に対してデジタルコンテンツを発行するコンテンツ発行サーバ 11 と、当該デジタルコンテンツの発行に用いられる「create コマンド（所定のコマンド）」及び「create 権（生成権）」を生成して管理するコマンド生成サーバ 3 とを備える。

ここで、デジタルコンテンツの発行は、コンテンツ発行サーバ 11 において生成されたデジタルコンテンツと、第 2 の IC カード 1 b に格納されている電子マネーとを交換することによって行われる。

詳述すると、デジタルコンテンツの発行は、コンテンツ発行サーバ 11 内に装填された第 1 の IC カード 1 a 内に一時的に格納されているデジタルコンテンツ（電子チケット等）が、第 2 の IC カード 1 b に転送され、第 2 の IC カード 1 b 内に一時的に格納されているデジタルコンテンツ（電子マネー）が、コンテンツ発行サーバ 11 に転送されることによって行われる。

この際、コマンド生成サーバ 3 から取得した create コマンドが実行されることによって、コンテンツ発行サーバ 11 と第 2 の IC カード 1 b との間のデジタルコンテンツの交換が行われる。create コマンドを実行するには、コマンド生成サーバ 3 で発行された create

e 権が必要となる。

コンテンツ発行サーバ 11 は、一時的にデジタルコンテンツを格納する第 1 の IC カード 1 a が装填されるインターフェイスを備えており、
create コマンドを実行することによって、デジタルコンテンツを、
5 第 2 の IC カード 1 b 内に転送するサービスを行うサーバである。

create コマンドは、図 11 に示すように、コンテンツ発行サーバ 11 からコマンド生成サーバ 3 に対して「登録要求」が送信された場合に、コマンド生成サーバ 3 によって登録が認められたコンテンツ発行サーバ 11 に対して発行される実行プログラムである。

10 また、図 12 に示すように、create コマンドは、第 1 の IC カード 1 a によって実行される度に、コマンド生成サーバ 3 に対して「認証要求」を送信し、当該 create コマンドに対応する create 権が存在するか否かについて、すなわち、当該 create 権が発行されているか否かについて照合（認証）する。

15 当該 create コマンドは、当該 create コマンドに対応する create 権が発行されている場合にのみ動作し、当該 create 権が発行されていない場合には、動作を拒否する。

なお、本実施形態では、図 12 に示すように、コンテンツ発行サーバ 11 は、コマンド生成サーバ 3 における認証結果について、コマンド生成サーバ 3 から送信される「ack (ok/reject)」によって確認することができる。

すなわち、コンテンツ発行サーバ 11 は、create コマンドを実行することにより、コマンド生成サーバ 3 に対して、コマンド生成要求（上述の認証要求）を送信し、当該コマンド生成要求に対してコマンド
25 生成サーバ 3 から ack (ok) を取得した場合に、デジタルコンテン

ツを生成することができる。

また、コンテンツ発行サーバ 11 は、デジタルコンテンツの生成に先
立って、コマンド生成サーバ 3 に対して登録処理を行い、create
コマンドを取得する必要がある。かかる登録処理によって、コマンド生
5 成サーバ 3 は、当該createコマンドに対するcreate権を発
行する。この発行されたcreate権は、登録サーバデータベース 3
1 において管理される。

また、コンテンツ発行サーバ 11 は、デジタルコンテンツを生成する
際、コマンド生成サーバ 3 との間で認証処理を行い、create権を
10 取得する必要がある。かかる認証処理において、コンテンツ発行サーバ
11 は、コマンド生成サーバ 3 に対して、コンテンツ生成要求（認証要
求）と、個人情報（サーバ情報）と、当該コンテンツ発行サーバ 11 自
身の署名データとを送信する。

また、コマンド生成サーバ 3 は、createコマンドを生成（発行）
15 して、コンテンツ発行サーバ 11 に対して送信するとともに、発行され
たcreateコマンドに対応するcreate権を発行して管理する
ものである。かかるcreate権の管理には、登録サーバデータベー
ス 31 に格納された登録サーバリスト 31 a が用いられる。

コマンド生成サーバ 3 は、コンテンツ発行サーバ 11 から「登録要求」
20 と「個人情報（サーバ情報）」と「署名データ」とを受信した場合、受
信した「個人情報（サーバ情報）」に基づいて当該コンテンツ発行サー
バ 11 の正当性を検証し、当該コンテンツ発行サーバ 11 がデジタルコ
ンテンツを生成する資格があると判断した場合は、登録サーバリスト 3
1 a に、当該コンテンツ発行サーバ 11 に係る「個人情報（サーバ情報）」
25 を登録し、createコマンドを発行して当該コンテンツ発行サーバ

1 1 へ送信する。

また、コマンド生成サーバ3は、コンテンツ発行サーバ11から、コンテンツ生成要求（認証要求）を受信した場合、当該コンテンツ生成要求に応じて、登録サーバリスト31aの照合（認証）を行い、認証結果
5 が肯定的であるコンテンツ発行サーバのみにack（ok）を返す。

（動作）

本実施形態に係るデータ通信方法（デジタルコンテンツの発行方法）について説明する。図13は、本実施形態に係るデジタルコンテンツの発行方法を示すシーケンス図である。

10 図13に示すように、ステップS1101において、コンテンツ発行サーバ11が、コマンド生成サーバ3に対して、「登録要求」と共に、「個人情報（サーバ情報）」及び「署名データ」を送信する。

ステップS1102において、コマンド生成サーバ3は、受信した「個人情報（サーバ情報）」に基づいて、当該コンテンツ発行サーバ11の
15 正当性を検証し、当該コンテンツ発行サーバ11がデジタルコンテンツを生成する資格があると判断した場合は、登録サーバリスト31aに、当該コンテンツ発行サーバ11に係る「個人情報（サーバ情報）」を登録し、ステップS1103において、createコマンドを当該コンテンツ発行サーバ11へ送信する。

20 ステップS1104において、コンテンツ発行サーバ11内に装填されている第1のICカード1aが、createコマンドを実行すると、ステップS1105において、当該createコマンドは、コマンド生成サーバ3に対して、「コンテンツ生成要求（認証要求）」と「個人情報（サーバ情報）」と「当該コンテンツ発行サーバ11自身の署名デ
25 ータ」とを送信する。

ステップS1106において、コマンド生成サーバ3は、当該createコマンドに対するcreate権が存在するか否かについて、登録サーバリスト31aにおいて照合する。

5 ステップS1107において、コマンド生成サーバ3は、当該認証結果を「ack(ok/reject)」として、コンテンツ発行サーバ11に送信する。

コマンド生成サーバ3から送信されたackの内容が「ok」である場合、ステップS1108において、コンテンツ発行サーバ11は、デジタルコンテンツ（例えば、電子チケット等）を生成する。

10 一方、コマンド生成サーバ3から送信されたackの内容が「reject」である場合、ステップS1109において、コンテンツ発行サーバ11は、デジタルコンテンツ（例えば、電子チケット等）の生成を行わず、createコマンド実行エラー処理を行う。

（変更例1）

15 なお、上述した第2の実施形態に対して、以下のような変更を採用することができる。図14及び図15は、変更例1に係るデジタルコンテンツ発行システムの構成を示すブロック図である。本変更例では、createコマンドとともに、create権自体が、コンテンツ発行サーバ11に対して発行される。

20 図14及び図15に示すように、本変更例に係るデジタルコンテンツ発行システムは、第1のICカード1aに対してデジタルコンテンツの発行を行うコンテンツ発行サーバ11と、デジタルコンテンツの発行に用いられるcreateコマンド及びcreate権を生成して管理するコマンド生成サーバ3'とを備える。

25 本変更例に係るコマンド生成サーバ3'は、createコマンドと

create権とを対応付けて管理する発行権管理部32を有する。

コンテンツ発行サーバ11は、コマンド生成サーバ3'から受信したcreateコマンド及びcreate権を、第1のICカード1a内に格納する。

- 5 createコマンドは、第1のICカード1aによって実行される度に、第1のICカード1a内において、当該createコマンドに対応付けられて格納されているcreate権が存在するか否かについて確認し、当該create権が存在する場合には、デジタルコンテンツを発行し、当該create権が存在しない場合には、create
- 10 コマンド実行エラー処理を行う。

本変更例に係るデータ通信方法（デジタルコンテンツの発行方法）について説明する。図16は、本変更例に係るデジタルコンテンツの発行方法を示すシーケンス図である。

- ステップS1201において、コンテンツ発行サーバ11は、コマンド生成サーバ3'に対して、「create権生成要求」と「個人情報（サーバ情報）」を送信する。
- 15

- ステップS1202において、コマンド生成サーバ3'は、「create権生成要求」の受信に応じて、受信した「個人情報」を検証して、当該コンテンツ発行サーバ11にデジタルコンテンツを生成する資格があるか否かを検証し、デジタルコンテンツを生成する資格があると判断した場合には、ステップS1203において、コンテンツ発行サーバ11に対して、create権及びcreateコマンドを送信する。
- 20

- ステップS1204において、コマンド生成サーバ3'から送信されたcreate権及びcreateコマンドは、コンテンツ発行サーバ11内の第1のICカード1a内に直接格納される。
- 25

ステップS 1 2 0 5において、コンテンツ発行サーバ1 1が、デジタルコンテンツを発行する場合は、createコマンドを実行する。

ステップS 1 2 0 6において、createコマンドは、第1のICカード1 a内のcreate権が存在するか否かを確認する。

- 5 第1のICカード1 a内にcreate権が存在すれば、コンテンツ発行サーバ1 1が、ステップS 1 2 0 7において、createコマンドを用いて、デジタルコンテンツを発行し、第1のICカード1 a内にcreate権が存在しない場合には、コンテンツ発行サーバ1 1が、ステップS 1 2 0 8において、createコマンド実行エラー処理を
10 行う。

(変更例 2)

- 図1 7及び図1 8を参照して、第2の実施形態の変更例2について説明する。図1 7及び図1 8は、本変更例に係るデジタルコンテンツ発行システムの構成を示すブロック図である。本変更例では、コンテンツ発行サーバ1 1の正当性の検証は、ソフトウェアによって行われるのではなく、物理的に行われる。
15

図1 7及び図1 8に示すように、本変更例に係るデジタルコンテンツ発行システムは、第1のICカード1 aに対してデジタルコンテンツの発行を行うコンテンツ発行サーバ1 1を具備している。

- 20 ここで、コンテンツ発行サーバ1 1には、最初からcreateコマンドが焼き込まれているICカード(ICチップ) 4が接続(装填)されており、当該コンテンツ発行サーバ1 1は、デジタルコンテンツを発行する際には、当該ICカード4にアクセスすることによって、createコマンドを呼び出して実行する。

- 25 ICカード4には、createコマンドが物理的に固定されており、

外部からの変更ができないようになっている。デジタルコンテンツ発行システムを変更する場合には、物理的に当該 IC チップ 4 を変更することで、コンテンツ発行サーバ 11 を変更する。

(変更例 3)

- 5 次いで、図 19 乃至図 21 を参照して、第 2 の実施形態の変更例 3 について説明する。図 19 及び図 20 は、本変更例に係るデジタルコンテンツ発行システムの構成を示すブロック図である。

図 19 及び図 20 に示すように、本変更例に係るデジタルコンテンツ発行システムは、第 1 の IC カード 1a に対してデジタルコンテンツの
10 発行を行うコンテンツ発行サーバ 11 と、デジタルコンテンツの発行に用いられる create コマンドを生成するコマンド生成サーバ 3” とを備える。

本変更例に係るコマンド生成サーバ 3” は、正当性が認証されたコンテンツ発行サーバ 11 (又は、第 1 の IC カード 1a) の ID を用いて、
15 create コマンドを暗号化して、当該コンテンツ発行サーバ 11 に対して送信する機能を有する。

図 21 を参照して、本変更例に係るデータ通信方法 (デジタルコンテンツの発行方法) について説明する。図 21 は、本変更例に係るデジタルコンテンツの発行方法を示すシーケンス図である。

- 20 図 21 に示すように、ステップ S13-1 において、コンテンツ発行サーバ 11 は、コマンド生成サーバ 3” に対して、「create コマンド生成要求」と共に、「個人情報 (コンテンツ発行サーバ 11 又は第 1 の IC カード 1a の ID を含む)」を送信する。

コマンド生成サーバ 3” は、ステップ S1302 において、「create
25 ate コマンド生成要求」に応じて、受信した「個人情報」に基づいて、

当該コンテンツ発行サーバ 11 の正当性について認証を行った後、当該
コンテンツ発行サーバ 11 にデジタルコンテンツを生成する資格がある
と判断した場合には、ステップ S 1303 において、コンテンツ発行サ
ーバ 11（又は、第 1 の IC カード 1 a）の ID を用いて、c r e a t e
5 e コマンドを暗号化する。

ステップ S 1304 において、コマンド生成サーバ 3” は、暗号化さ
れた c r e a t e コマンドを、コンテンツ発行サーバ 11 に対して送信
する。

コンテンツ発行サーバ 11 は、この暗号化された c r e a t e コマン
ドを受け取り、第 1 の IC カード 1 a 内に直接格納する。第 1 の IC カ
ード 1 a は、当該コンテンツ発行サーバ 11 に係る個人情報から、当該
10 コンテンツ発行サーバ 11 の ID を抽出する。

ステップ S 1305 において、第 1 の IC カード 1 a は、抽出したコ
ンテンツ発行サーバ 11 の ID（又は、第 1 の IC カード 1 a の ID）
15 を用いて、格納している c r e a t e コマンドの復号を行う。

ステップ S 1306 において、第 1 の IC カード 1 a は、復号された
create コマンドを実行し、デジタルコンテンツを発行する。この結果、正
当性が認証されたコンテンツ発行サーバ 11 のみに、c r e a t e コマ
ンドを発行することが可能となる。

20

産業上の利用可能性

以上説明したように、本発明によれば、外部の端末装置やサーバのコ
マンドを用いることなく、IC カード内部に備えられたアトミックなコ
マンドを用いて、デジタルコンテンツの暗号化処理や送信処理や交換処
25 理を行うことから、外部の端末装置やサーバ側からの不正な操作による

影響を回避することができ、外部の端末装置やサーバのセキュリティー環境によらず、安全なデジタルコンテンツの送信処理（又は、交換処理）を行うことができる。

- この結果、I Cカード間で直接通信を行う通信プラットフォーム上で、
- 5 デジタルコンテンツを送信（又は、交換）する際に、送受信者及び悪意のある第三者による複製や紛失を回避することができる。

請 求 の 範 囲

1. 第 1 のデジタルコンテンツを格納するホルダー部と、
前記第 1 のデジタルコンテンツに対応付けられた鍵情報を含む証明書
5 データを格納する証明書データ格納部と、
暗号処理部と、
実行処理部とを備え、
前記実行処理部は、所定のトリガー信号を受信すると、所定のコマン
ドを実行し、
10 前記実行処理部によって実行された前記所定のコマンドは、
前記実行処理部に、前記第 1 のデジタルコンテンツの送信前における
I C カードの状態を記憶させ、
前記暗号化処理部に、前記第 1 のデジタルコンテンツに対応付けられ
た前記鍵情報に基づいて、該第 1 のデジタルコンテンツの暗号化処理を
15 行わせ、
暗号化された前記第 1 のデジタルコンテンツの受信処理が完了した旨
を通知するコミット命令を送信先装置から受信した場合、前記ホルダー
部から前記第 1 のデジタルコンテンツを消去し、
前記第 1 のデジタルコンテンツの送信処理が中断された場合、前記実
20 行処理部に記憶されている前記 I C カードの状態への復帰処理を行うこ
とを特徴とする I C カード。
2. 前記実行処理部によって実行された前記所定のコマンドは、
前記コミット命令を受信した場合、前記送信先装置に対して第 2 のデ
ジタルコンテンツの送信要求を送信し、
25 前記第 2 のデジタルコンテンツの受信処理が完了した場合、前記ホル

ダー部から前記第 1 のデジタルコンテンツを消去することを特徴とする請求項 1 に記載の IC カード。

3. 前記第 1 のデジタルコンテンツの送信に先だって、前記送信先装置から該送信先装置の証明書データを取得し、該証明書データに基づいて該送信先装置の正当性を認証する認証部を具備し、

前記実行処理部は、前記送信先装置の正当性が認証された場合に、前記所定のコマンドを実行することを特徴とする請求項 1 に記載の IC カード。

4. 前記認証部は、前記送信先装置との間のセッションを識別するセッション ID とセッションモードとに応じて、前記ホルダー部に格納されている前記第 1 のデジタルコンテンツへのアクセスレベルを設定することを特徴とする請求項 3 に記載の IC カード。

5. 前記認証部は、前記第 1 のデジタルコンテンツの送信に先だって、前記証明書データ格納部に格納されている前記証明書データを前記送信先装置に対して送信し、前記送信先装置から該証明書データの正当性が認証された旨を通知する認証確認通知を取得し、

前記実行処理部は、前記認証確認通知が取得された場合に、前記所定のコマンドを実行することを特徴とする請求項 3 に記載の IC カード。

6. IC カードに格納されている第 1 のデジタルコンテンツを送信先装置に送信する端末装置であって、

入力された操作信号に基づいて、所定のトリガー信号を、前記 IC カードに対して出力する制御部を具備し、

前記 IC カードの実行処理部は、前記所定のトリガー信号に応じて、所定のコマンドを実行し、

- 25 前記実行処理部によって実行された前記所定のコマンドは、

前記実行処理部に、前記第 1 のデジタルコンテンツの送信前における前記 IC カードの状態を記憶させ、

前記 IC カードの暗号化処理部に、前記第 1 のデジタルコンテンツに対応付けられた鍵情報に基づいて、該第 1 のデジタルコンテンツの暗号化処理を行わせ、

暗号化された前記第 1 のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を前記送信先装置から受信した場合、前記 IC カードのホルダー部から前記第 1 のデジタルコンテンツを消去し、

前記第 1 のデジタルコンテンツの送信処理が中断された場合、前記実行処理部に記憶されている前記 IC カードの状態への復帰処理を行うことを特徴とする端末装置。

7. 前記実行処理部によって実行された前記所定のコマンドは、

前記コミット命令を受信した場合、前記送信先装置に対して第 2 のデジタルコンテンツの送信要求を送信し、

前記第 2 のデジタルコンテンツの受信処理が完了した場合、前記ホルダー部から前記第 1 のデジタルコンテンツを消去することを特徴とする請求項 6 に記載の端末装置。

8. 前記 IC カードから前記送信先装置に前記第 1 のデジタルコンテンツを送信した後、所定の待機時間を経過するまでの間に、該送信先装置から応答がない場合、前記第 1 のデジタルコンテンツの送信処理が中断された旨を前記 IC カードに通知する通信監視部を具備することを特徴とする請求項 6 に記載の端末装置。

9. 前記 IC カードと前記送信先装置との間で確立されているセッションを識別するセッション ID とセッションモードとに応じて設定されたアクセスレベルに基づいて、前記ホルダー部から前記第 1 のデジタル

コンテンツに関する情報を読み出して表示する表示部を具備することを特徴とする請求項 6 に記載の端末装置。

10. ICカードに格納されている第 1 のデジタルコンテンツを送信先装置に送信するデータ通信方法であって、

- 5 前記 ICカードが、所定のトリガー信号を受信すると、所定のコマンドを実行する工程と、

前記第 1 のデジタルコンテンツの送信前における ICカードの状態を記憶する工程と、

- 10 前記第 1 のデジタルコンテンツに対応付けられた鍵情報に基づいて、
該第 1 のデジタルコンテンツの暗号化処理を行う工程と、

暗号化された前記第 1 のデジタルコンテンツの受信処理が完了した旨を通知するコミット命令を前記送信先装置から受信した場合、前記 ICカードのホルダー部から前記第 1 のデジタルコンテンツを消去する工程と、

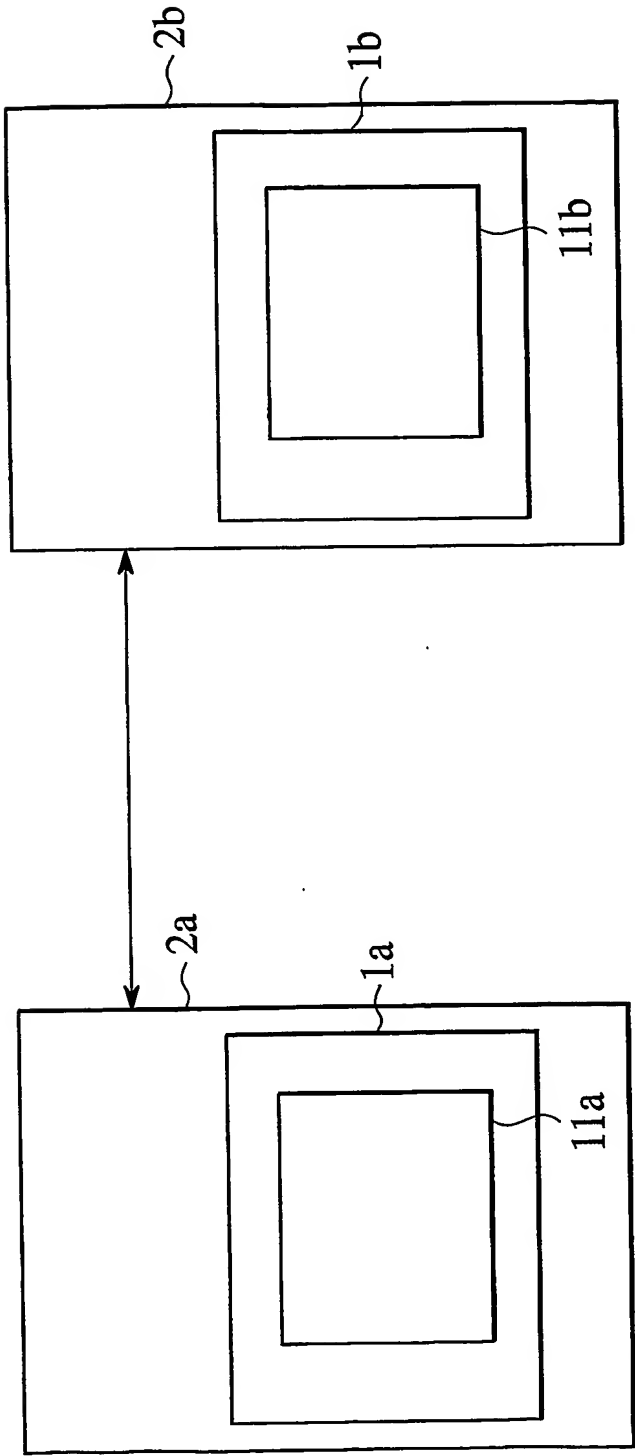
- 15 前記第 1 のデジタルコンテンツの送信処理が中断された場合、記憶されている前記 ICカードの状態への復帰処理を行う工程とを有することを特徴とするデータ通信方法。

11. 前記コミット命令を受信した場合、前記送信先装置に対して第 2 のデジタルコンテンツの送信要求を送信する工程と、

- 20 前記第 2 のデジタルコンテンツの受信処理が完了した場合、前記ホルダー部から前記第 1 のデジタルコンテンツを消去する工程とを有することを特徴とする請求項 10 に記載のデータ通信方法。

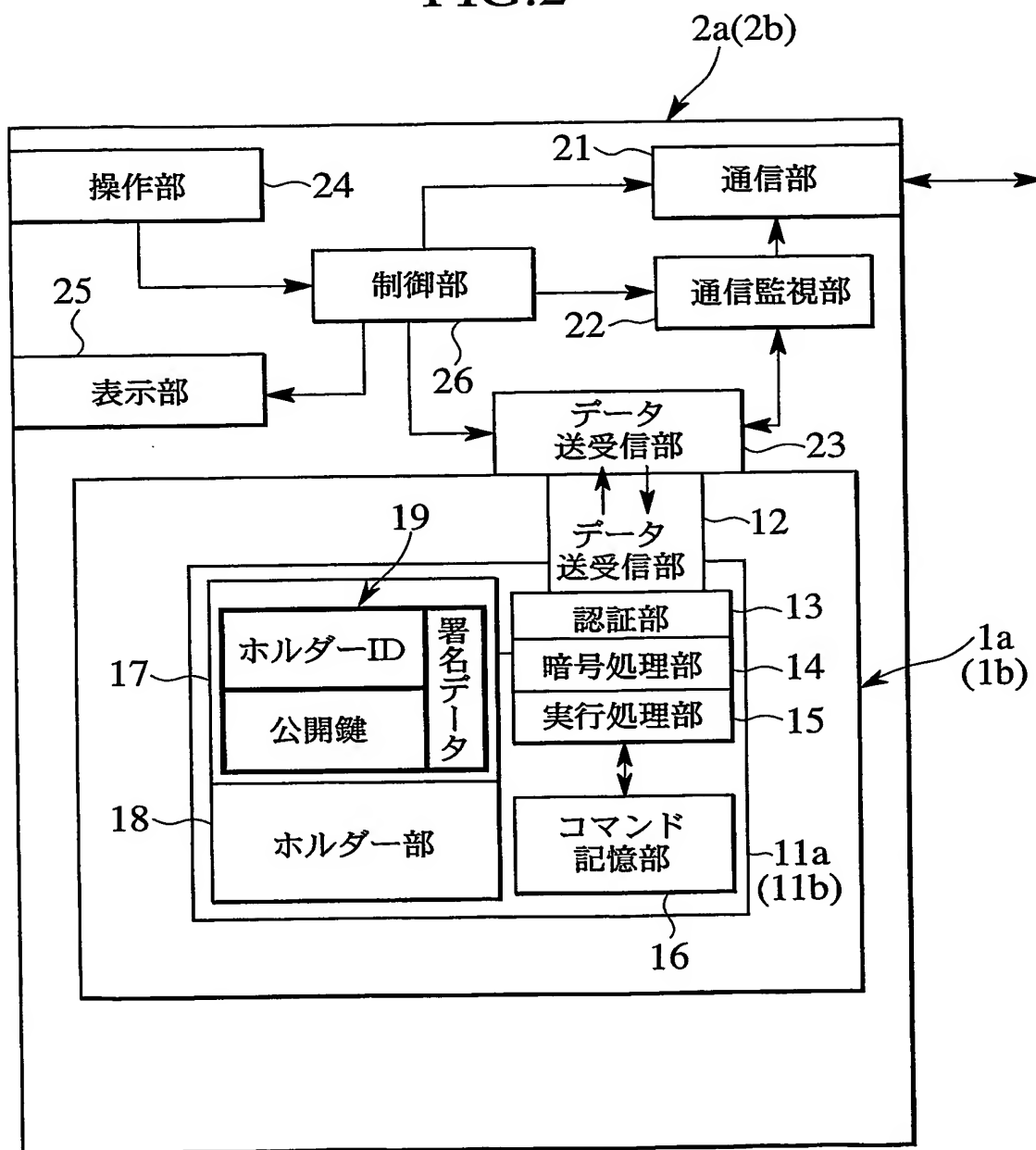
12. 前記 ICカードが装填された端末装置が、入力された操作信号に基づいて、前記所定のトリガー信号を、前記 ICカードに対して出力
25 する工程を有することを特徴とする請求項 10 に記載のデータ通信方法。

FIG.1



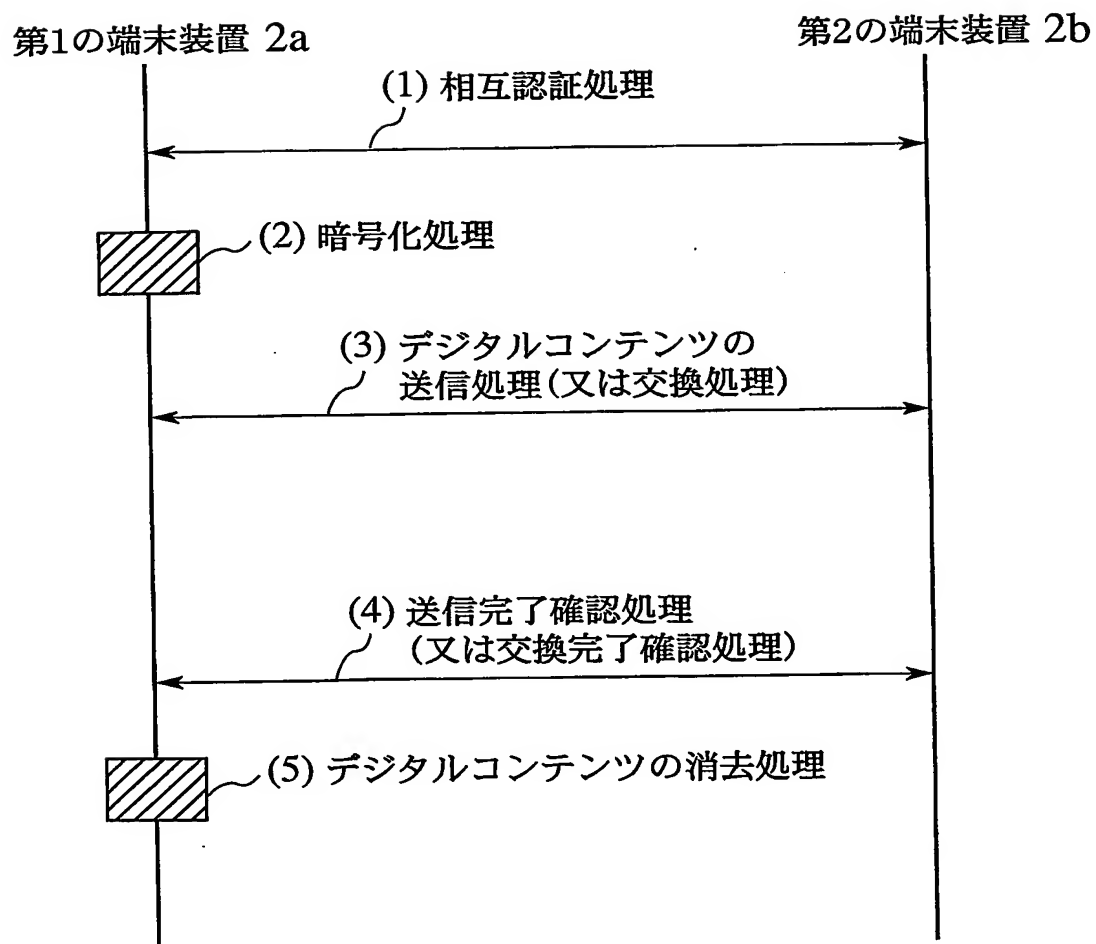
2/15

FIG.2



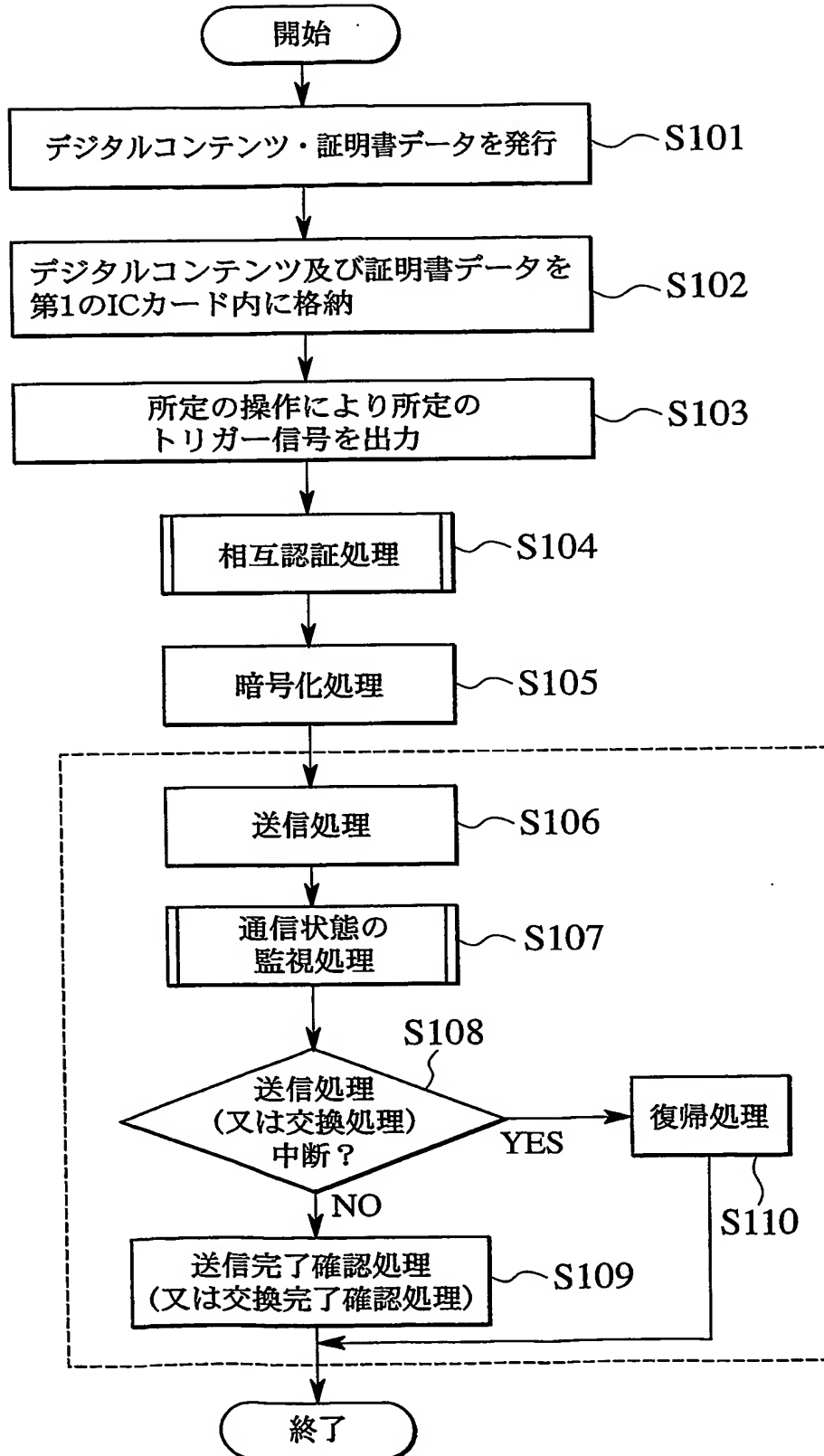
3/15

FIG.3



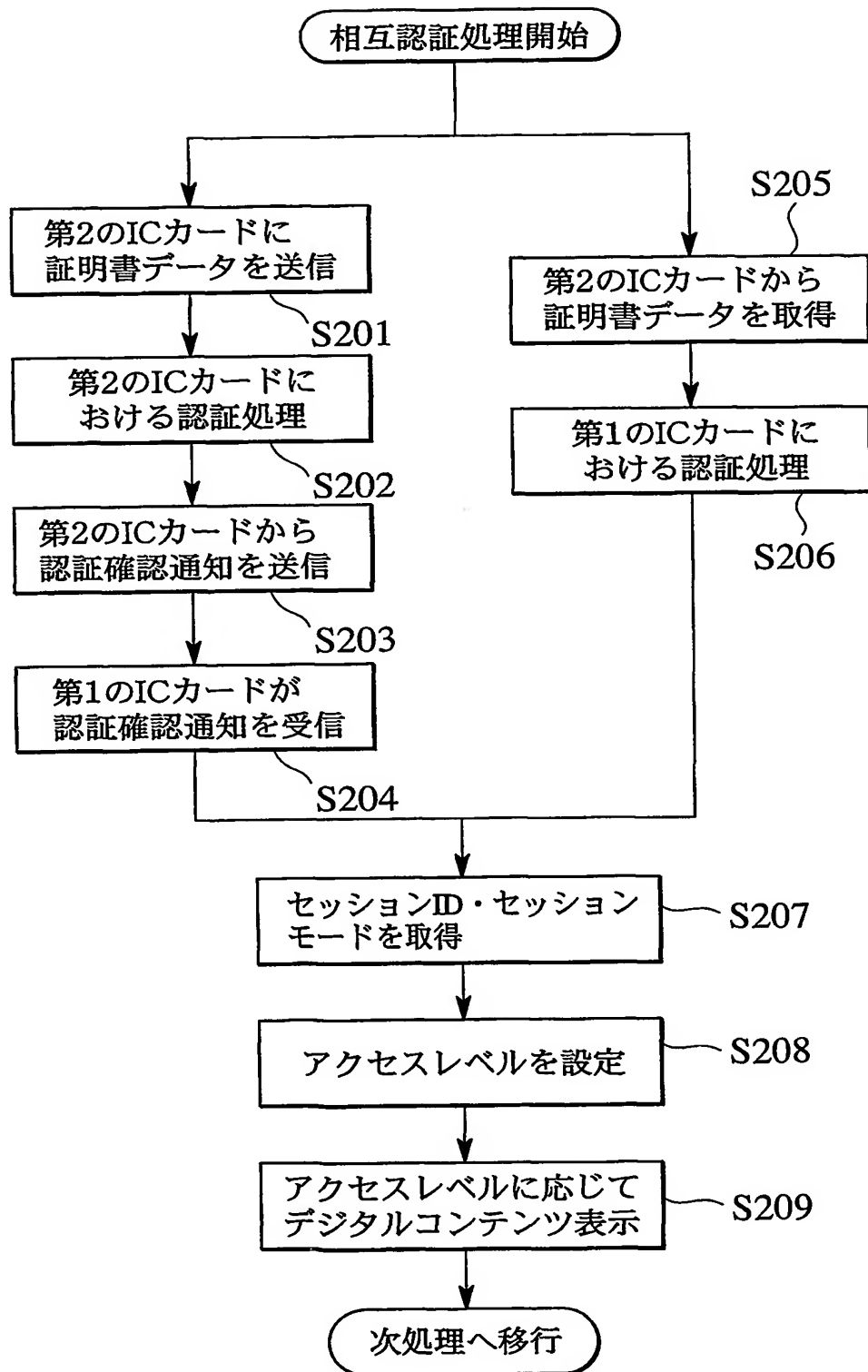
4/15

FIG.4



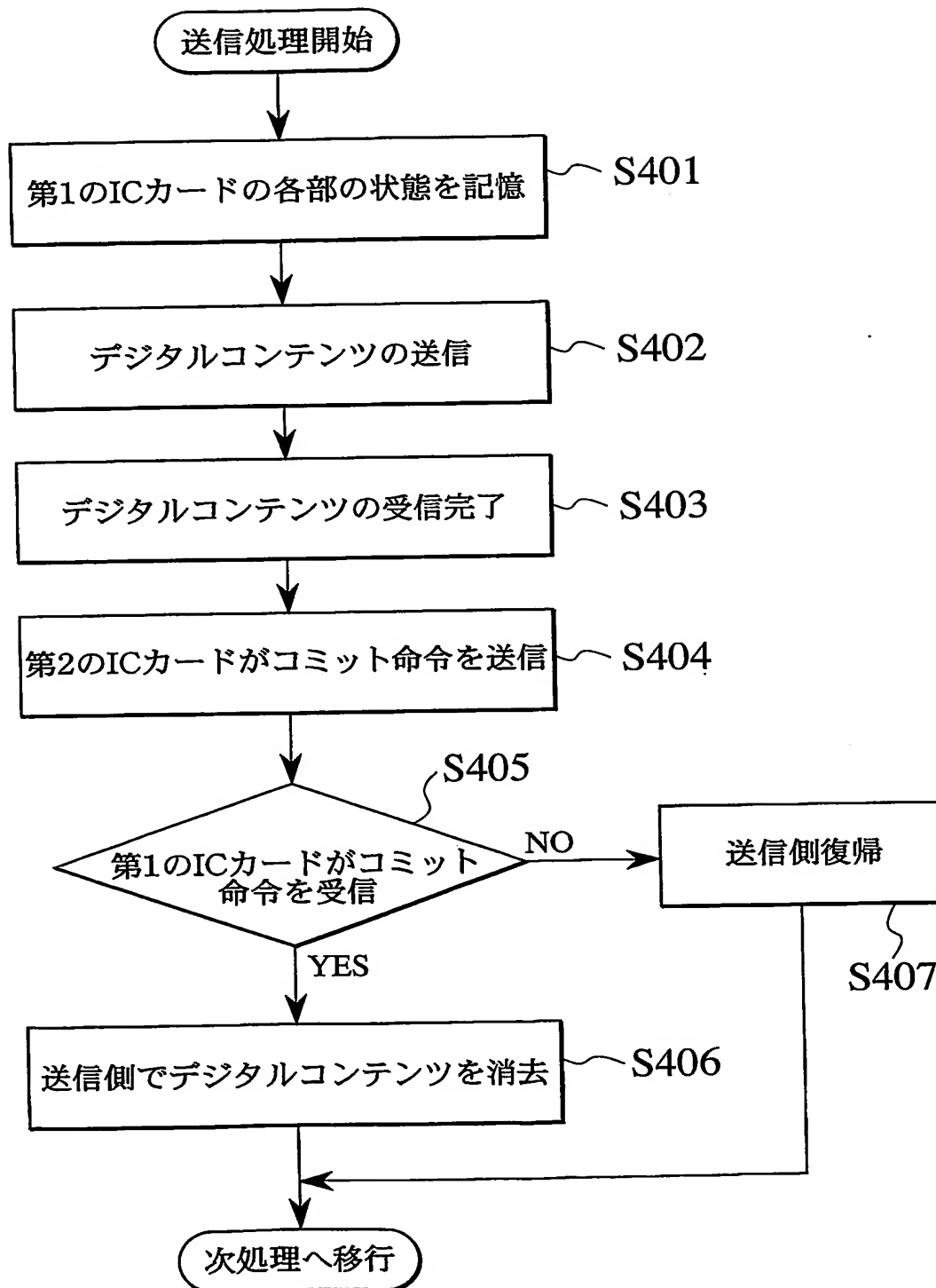
5/14

FIG.5



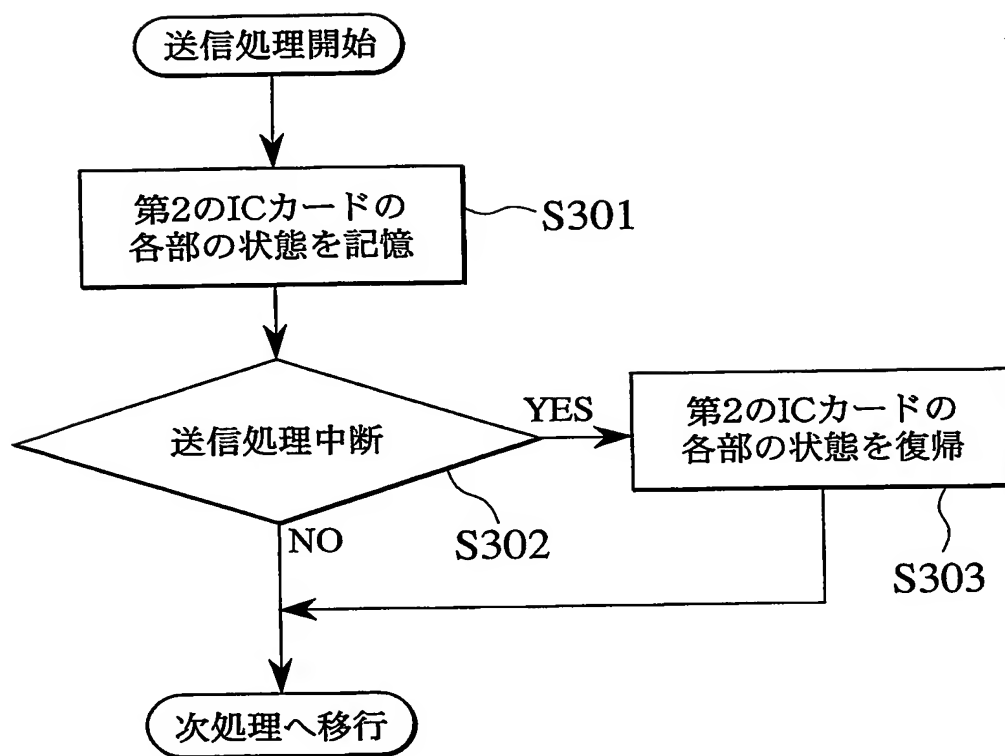
6/15

FIG.6



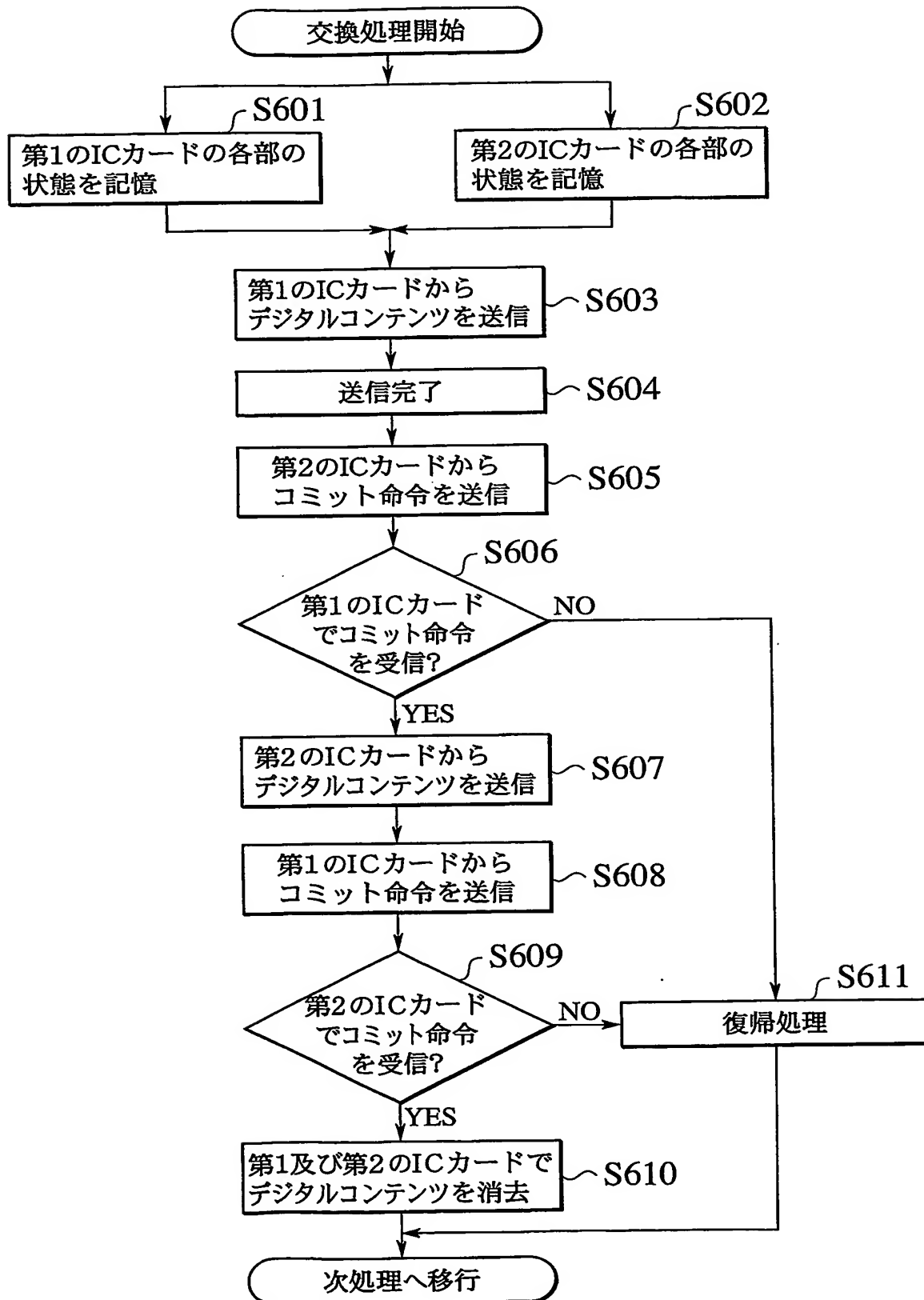
7/15

FIG.7



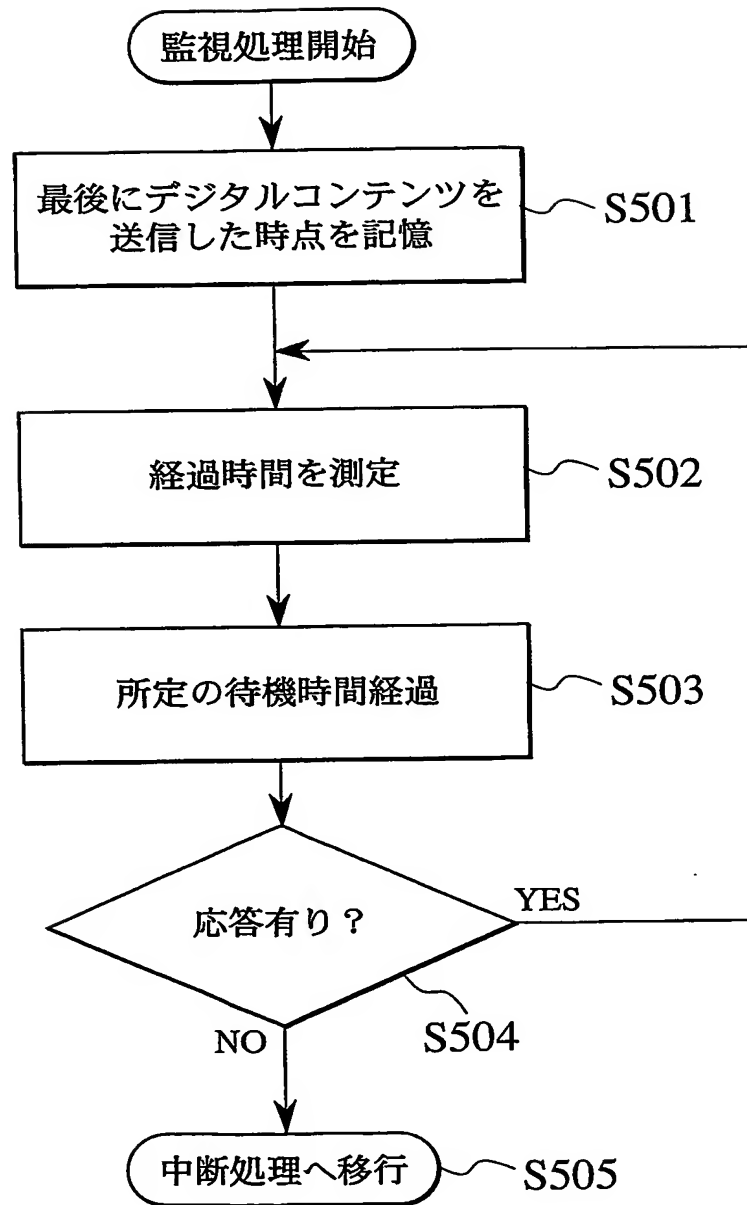
8/15

FIG.8



9/15

FIG.9



10/15

FIG.10

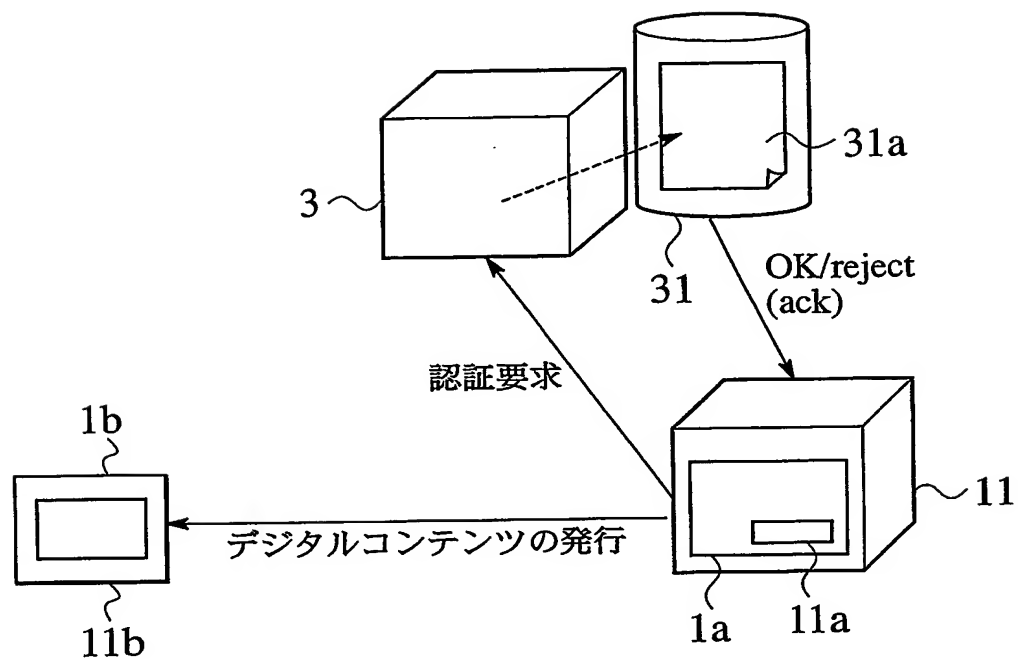
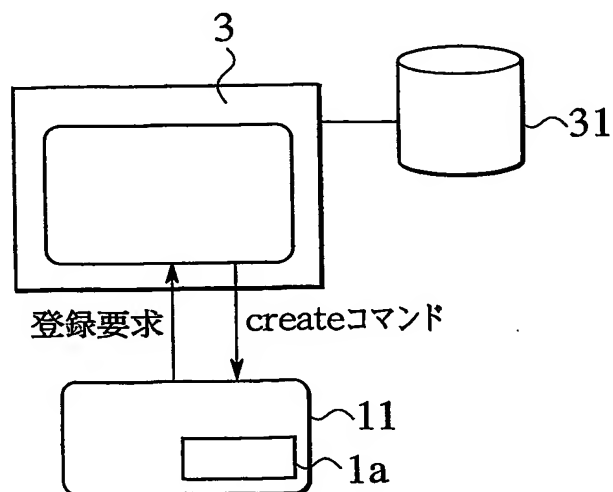
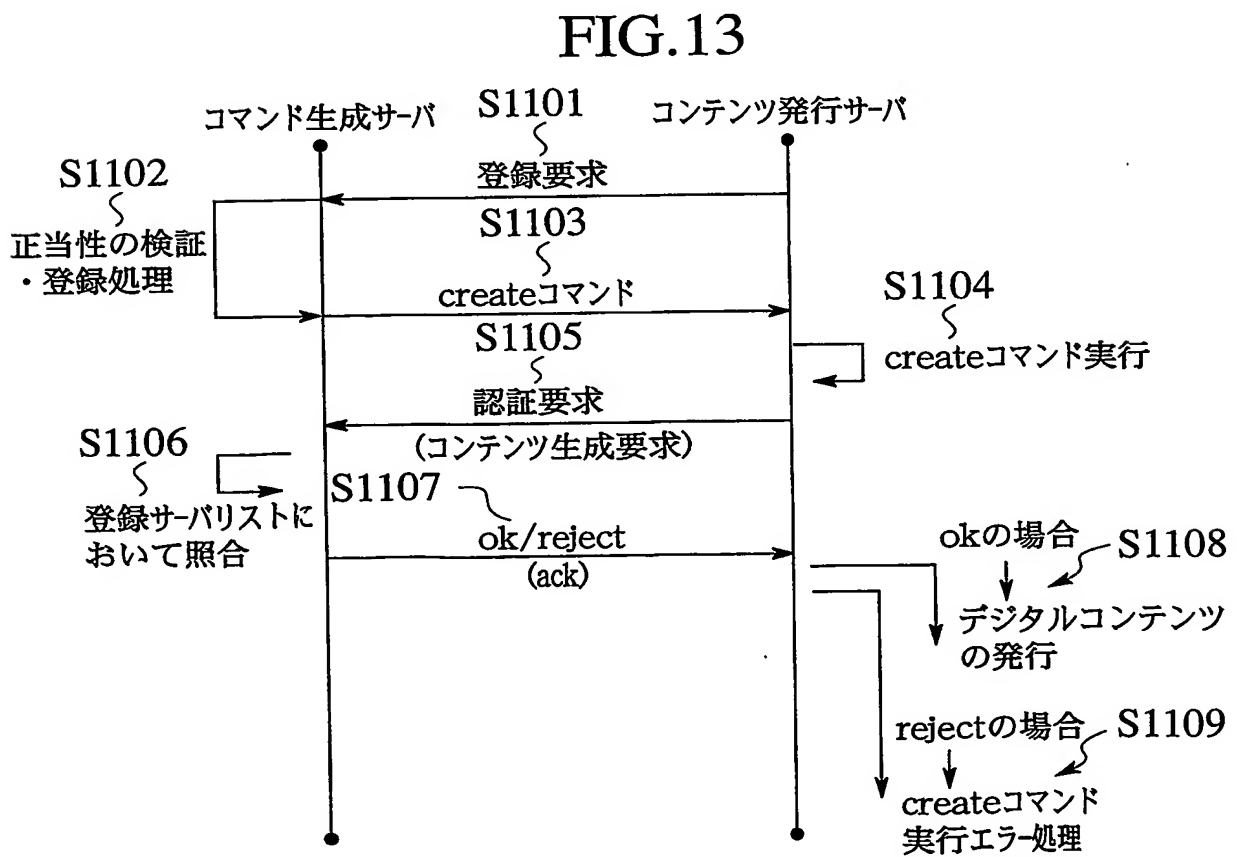
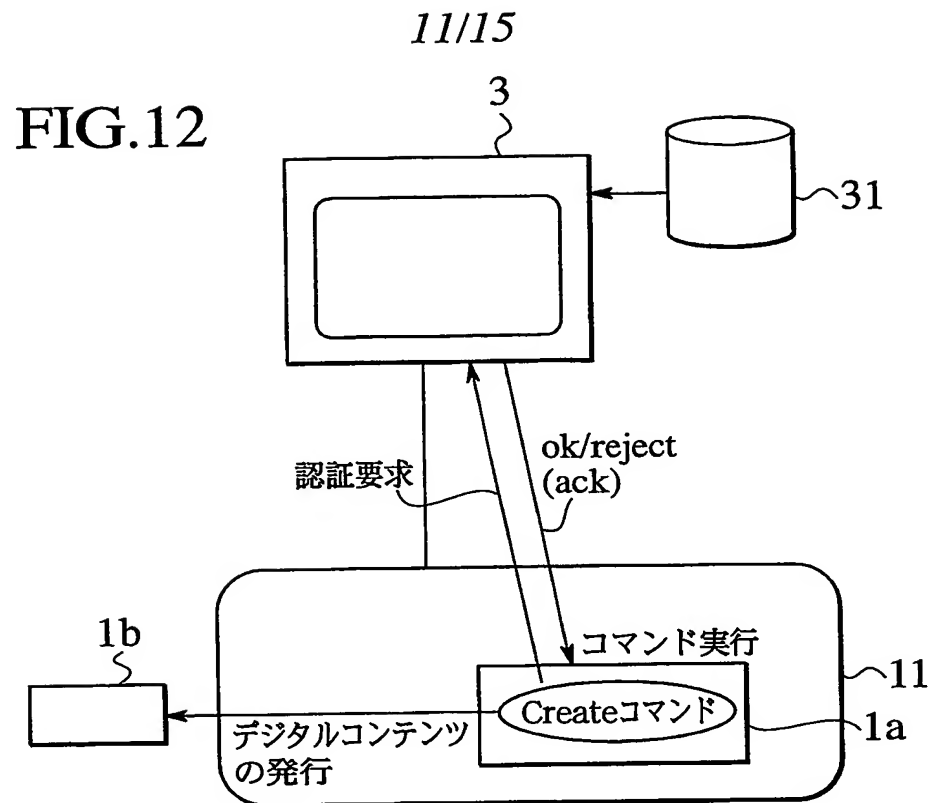


FIG.11





12/15

FIG.14

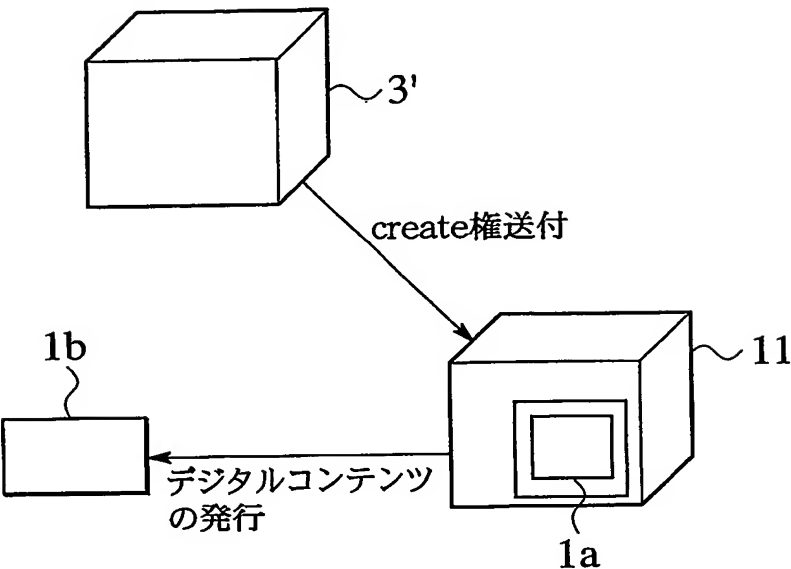
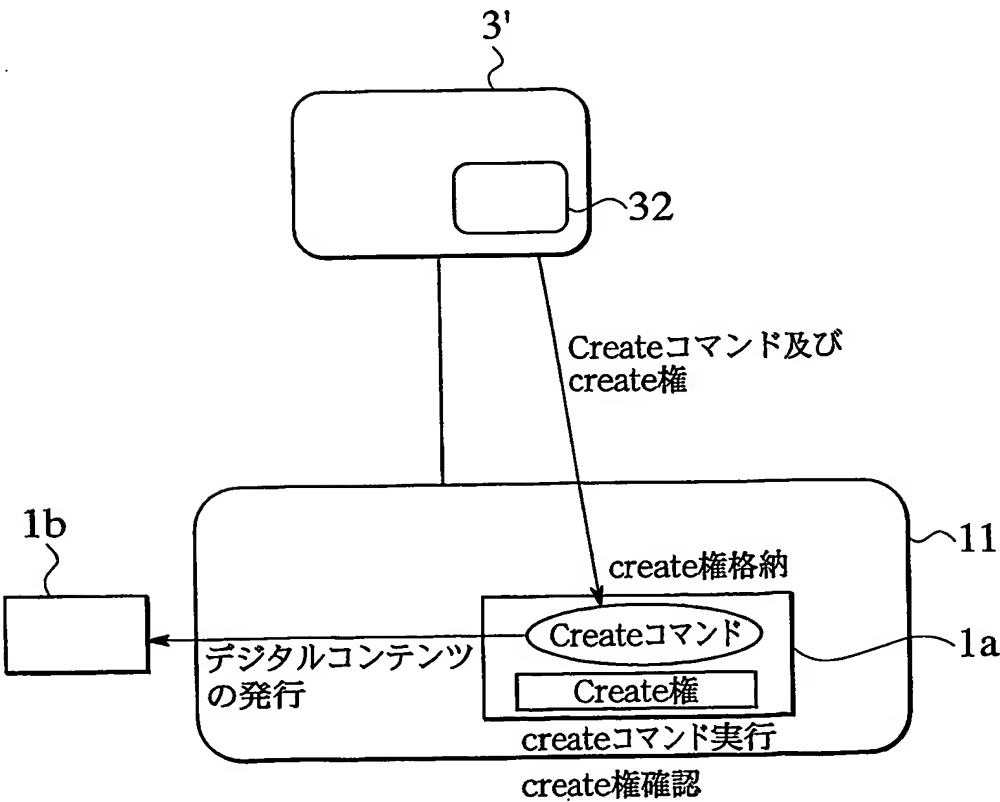


FIG.15



13/15

FIG.16

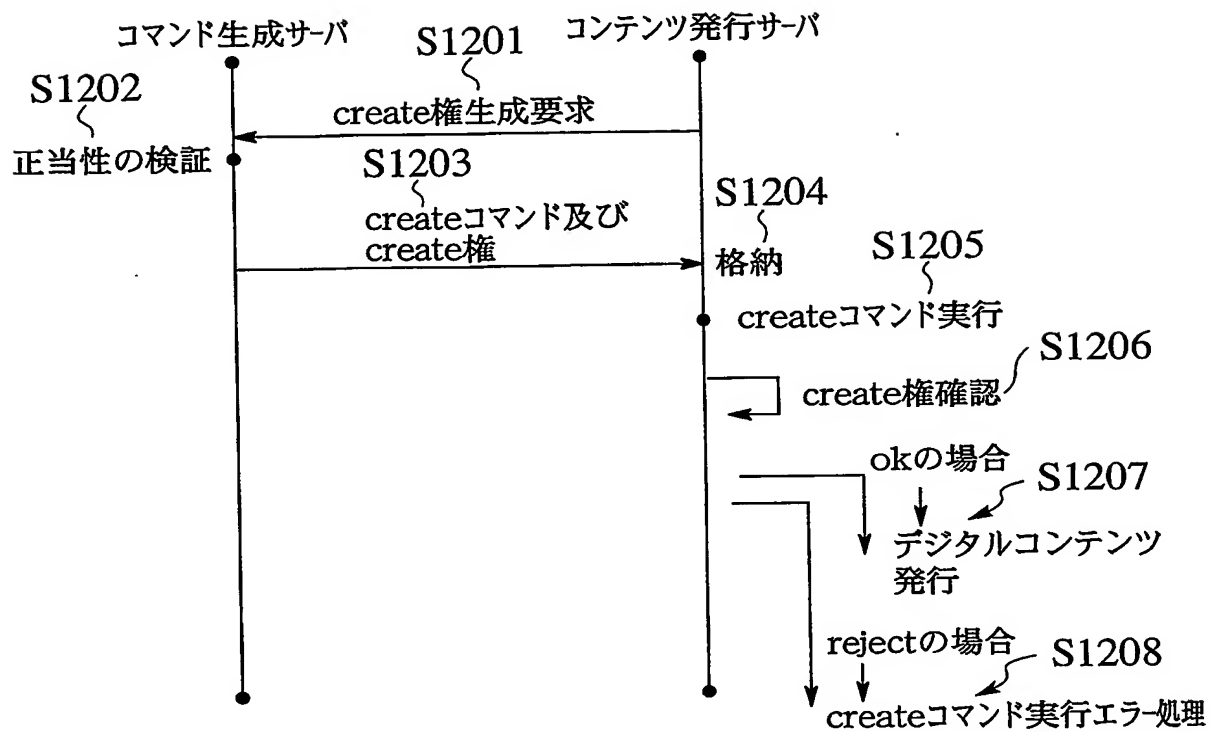
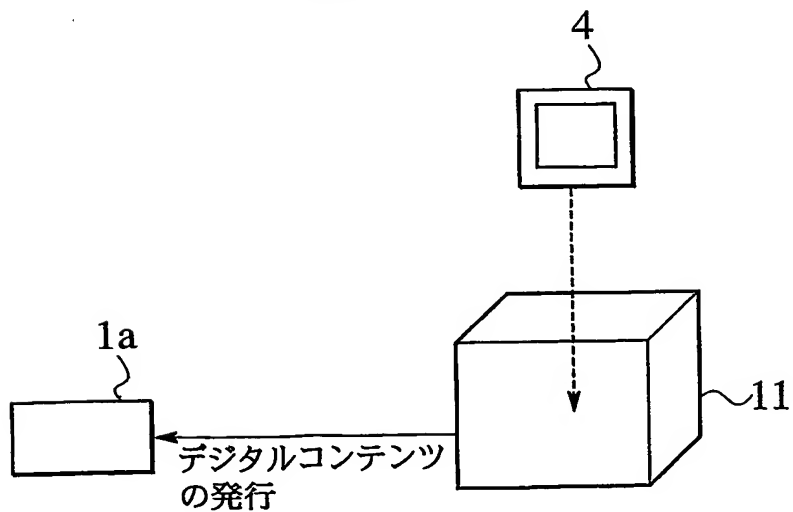


FIG.17



14/15

FIG.18

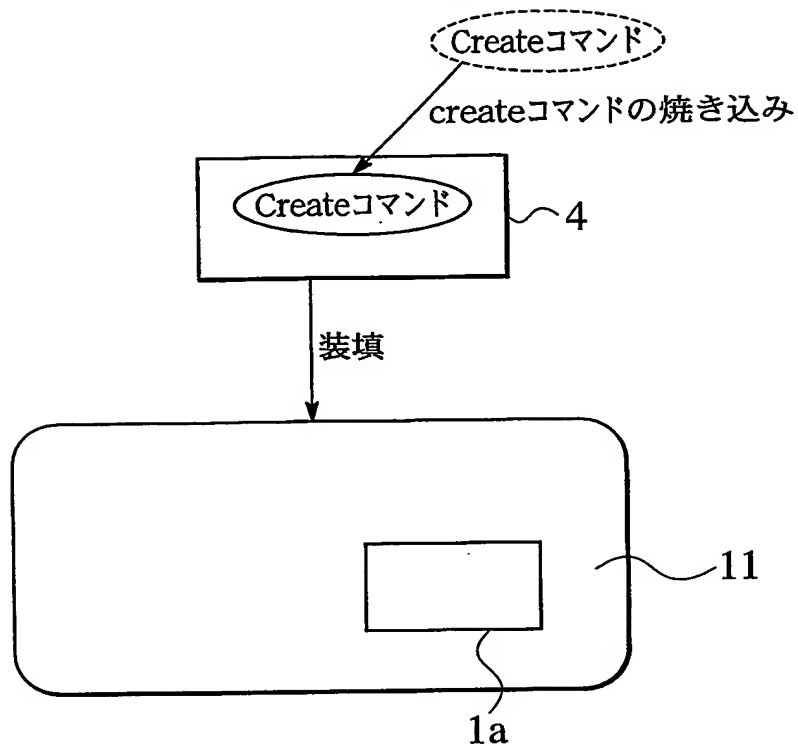
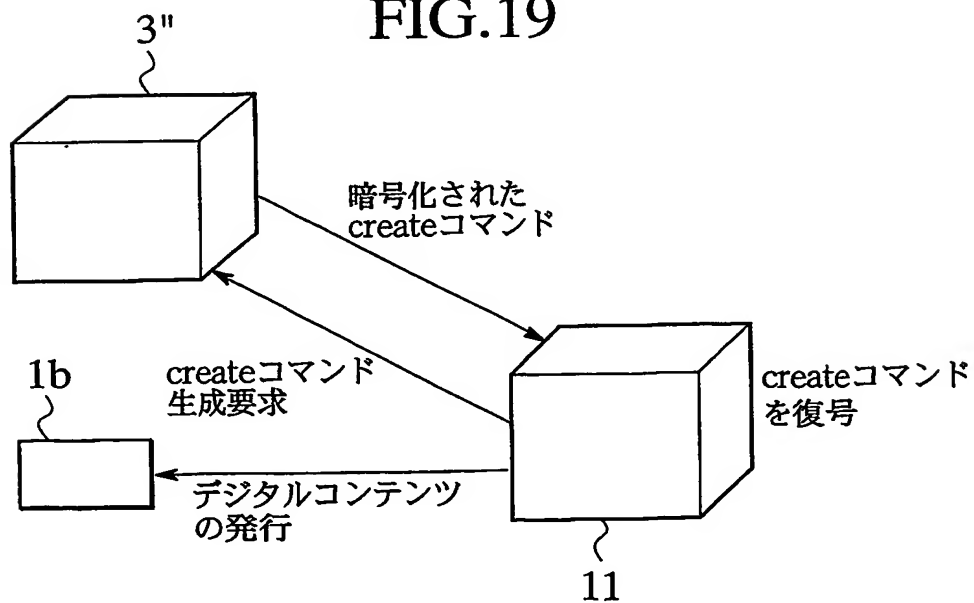


FIG.19



15/15

FIG.20

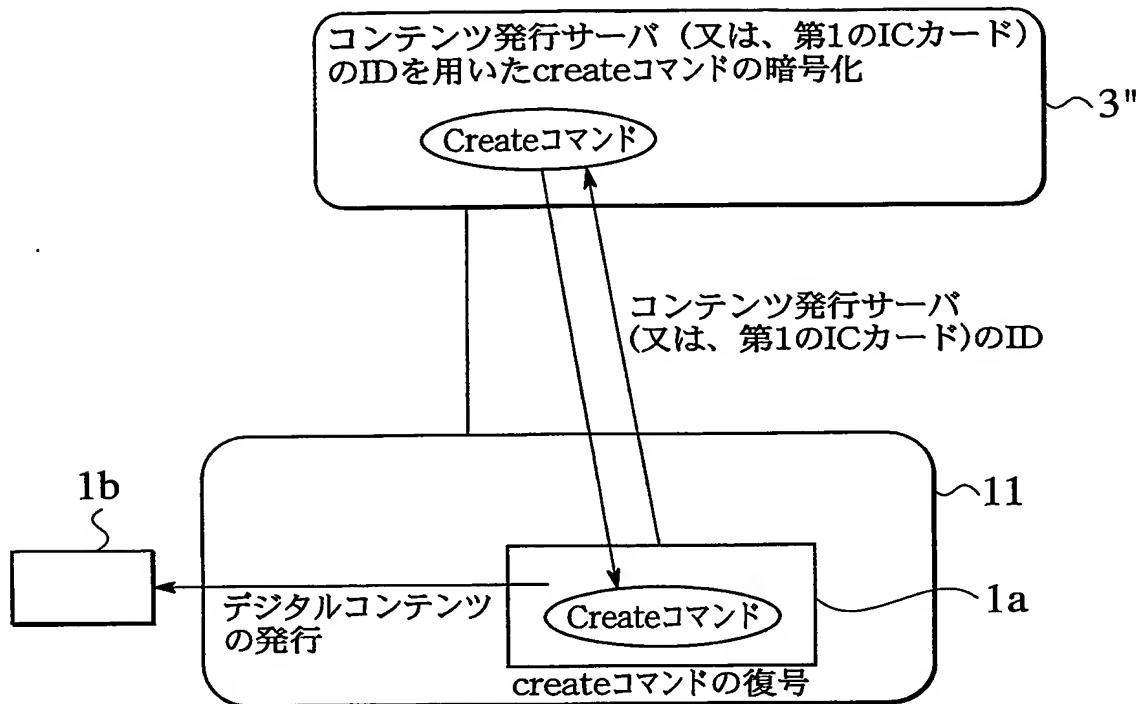
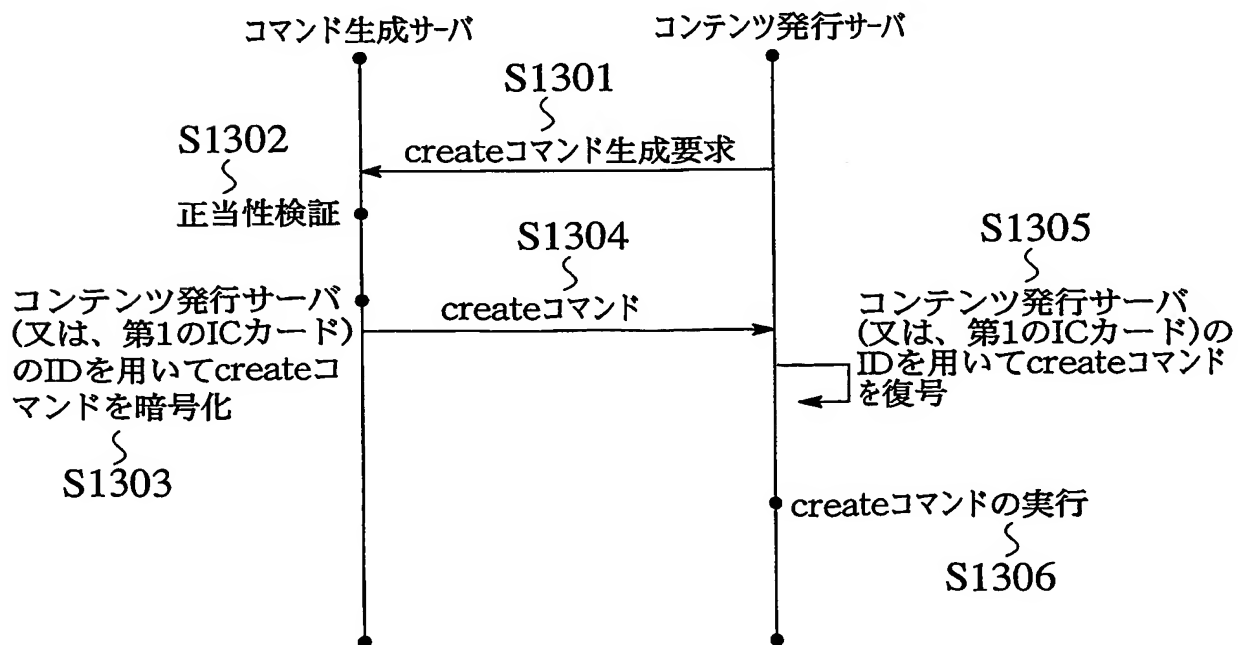


FIG.21



INTERNATIONAL SEARCH REPORT

International Application No.
PCT/JP03/07250

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, G06F17/60, G06K17/00, G06K19/10, G06F15/00,
G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, G06F17/60, G06K17/00, G06K19/10, G06F15/00,
G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2001-84177 A (Matsushita Electric Industrial Co., Ltd.), 30 March, 2001 (30.03.01), All pages; all drawings (Family: none)	1, 3-6, 8-10, 12 2, 7, 11
Y A	JP 2002-101087 A (Hitachi, Ltd.), 05 April, 2002 (05.04.02), All pages; all drawings & US 2002/34306 A1	1, 3-6, 8-10, 12 2, 7, 11
Y	JP 2001-333371 A (Matsushita Electric Industrial Co., Ltd.), 30 November, 2001 (30.11.01), All pages; all drawings & WO 01/89210 A1	1, 3-6, 8-10, 12

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:
 "A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier document but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
29 August, 2003 (29.08.03)Date of mailing of the international search report
09 September, 2003 (09.09.03)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/JP03/07250

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-243707 A (Sony Corp.), 07 September, 2001 (07.09.01),	1, 3-6, 8-10, 12
A	All pages; all drawings (Family: none)	2, 7, 11
A	"TRONWARE VOL.73", Personal Media Corp., 10 February, 2002 (10.02.02), Vol.13, No.1, whole No. 73, pages 48 to 56	1-12

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F17/60, G06K17/00,
G06K19/10, G06F15/00, G09C1/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F17/60, G06K17/00,
G06K19/10, G06F15/00, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926 - 1996
日本国公開実用新案公報 1971 - 2003
日本国登録実用新案公報 1994 - 2003
日本国実用新案登録公報 1996 - 2003

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2001-84177 A (松下電器産業株式会社) 2001. 03. 30, 全頁, 全図 (ファミリーなし)	1, 3-6, 8-10, 12
A		2, 7, 11
Y	JP 2002-101087 A (株式会社日立製作所) 2002. 04. 05, 全頁, 全図 & US 2002/34306 A1	1, 3-6, 8-10, 12
A		2, 7, 11

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に関する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

29. 08. 03

国際調査報告の発送日

09.09.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

奥村 元宏

5 N

3 0 4 4

電話番号 03-3581-1101 内線 3585

C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2001-333371 A (松下電器産業株式会社) 2001. 11. 30, 全頁, 全図 & WO 01/89210 A1	1, 3-6, 8-10, 12
A		2, 7, 11
Y	JP 2001-243707 A (ソニー株式会社) 2001. 09. 07, 全頁, 全図 (ファミリーなし)	1, 3-6, 8-10, 12
A		2, 7, 11
A	"TRONWARE VOL. 73", パーソナルメディア株式会社, 2002. 02. 10, 第13巻, 第1号, 通巻73号, pp. 48-56	1-12